Fraunhofer

DATA SOVEREIGNTY AND DATA ECONOMY

TWO REPULSIVE FORCES?

universität Witten/Herdecke
Institute for Digital Transformation in Healthcare

KIT Karlsruhe Institute of Technology

CRITICAL INFORMATION INFRASTRUCTURES RESEARCH GROUP

T · · Systems ·

Data Sovereignty and Data Economy —Two Repulsive Forces?

Position Paper

DaWID

Data-Driven Value Creation Platform
for Interactive, Assisting Service Systems

SPONSORED BY THE

Federal Ministry
of Education
and Research

The objective of this paper is to illuminate the interplay of datasovereignty and data economy. To understand this interaction, it is important to consider a holistic approach consisting of data sovereignty, data economy, data rights, and data ethics. In this context, we identify and elaborate ten potential areas of tension.

Authors

Florian Lauf
Simon Scheider
Sven Meister

Fraunhofer ISST

Marija Radic
Philipp Herrmann
Max Schulze

Fraunhofer IMW

André T. Nemat
Sarah J. Becker
Marcel Rebbert

Universität Witten/Herdecke – Institute for Digital Transformation in Healthcare

Constantin Abate
Ralf Konrad

T-Systems

Jan Bartsch
Tobias Dehling
Ali Sunyaev

KIT Karlsruhe Institute of Technology

Critical Information Infrastructures Research Group

Publisher

Fraunhofer Institute for Software and Systems Engineering ISST
Emil-Figge-Str. 91
44227 Dortmund
Germany
DOI: 10.24406/isst-n-634865
Email: info@dawid-projekt.de

Image sources

p.4: ©3dkombinat - Fotolia
p.6: ©ryzhi - stock.adobe.com
p.8: ©sdecoret - Depositphotos
p.14: ©luckybusiness - stock.adobe.com
p.26: ©everythingposs - Depositphotos
p.29: ©stori - Depositphotos

Links

www.dawid-projekt.de
www.interaktive-technologien.de/projekte/dawid

Layout

Lena Sodenkamp, Fraunhofer ISST

May 2021

Table of Contents

1 Executive Summary

When thinking of a company's assets, typically tangible assets such as factories, inventory, cash, or intangible assets like brands, patents, or intellectual property come to mind. However, over the past decades, a new type of asset has gained importance: data. More and more data is gathered, analyzed, and used to either allow for better informed business decisions or to develop entirely new business models. The so-called data economy is based on using data to create value (Opher et al. 2016).

In this type of economy, citizens play a crucial role because on the most granular level, they are often the providers of data. However, from a citizen's perspective, data flows are usually not transparent and there is a lack of instruments for informational self-determination. This raises the fundamental question whether the autonomy of a data subject is given in the first place: The autonomy to make decisions about who accesses, processes, or stores data, and to move around in the data space in a self-determined, well-informed manner (Federal Government 2021).

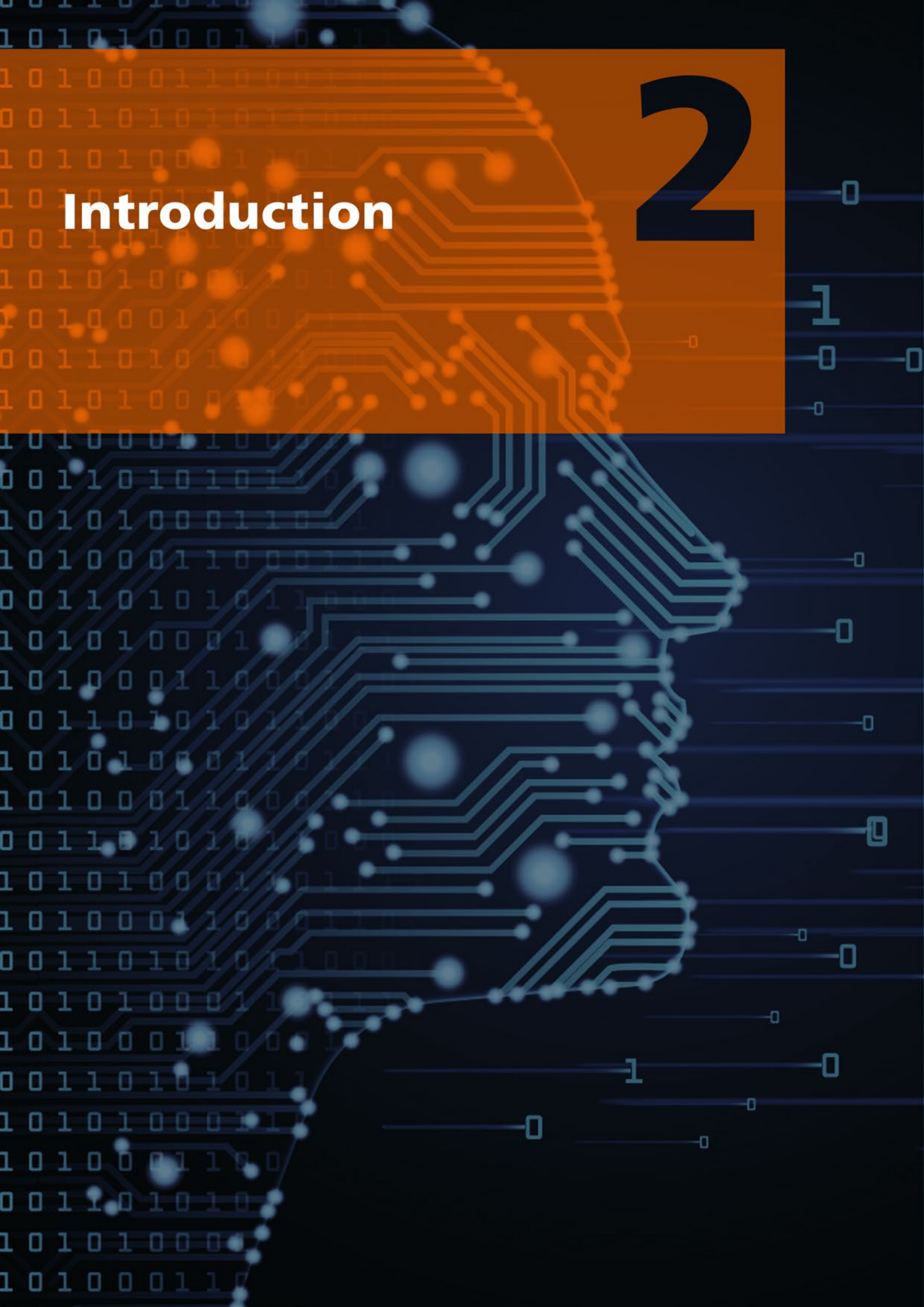
The objective of this paper is to illuminate the interplay of data sovereignty and data economy. To understand this interaction, it is important to consider a holistic approach consisting of data sovereignty, data economy, data rights, and data ethics.

In this context, we identify and elaborate ten potential areas of tension: First, data processing and data value chains lead to the loss of claims of individual data providers to the final product ('data processing'). But at this point, however, it is vital to consider particularly the data provider (i.e., the citizen). Second, data economies might pretend to ensure data sovereignty of citizens albeit behaving differently ('manipulation'). For this reason, codes of conduct are necessary, and their guidelines must be enforced at all levels. Third, data scandals create mistrust among citizens, which is why companies are increasingly constrained to establish trust in order to retain their customers ('mistrust'). Consequently, fourth, a declared goal of companies acting responsibly should be to maintain data sovereignty of their customers by developing their business models accordingly ('responsibility'). Fifth, complications arise when the data source is anonymized ('anonymity'). In such cases, pseudonymization via data trustees could be a solution. Sixth, high switching costs for citizens as well as a high number of missing alternative services hinder citizens to switch providers ('lock-in effects'). Hence, overarching interoperability and easier data portability would meet the citizen's needs. Seventh, the fact, that there is no existing data ownership right and data is an intangible asset, leads to a complicated handling ('intangibility'). Eighth, many citizens are not aware of their data having value, or they face difficulties weighting the risks of data sharing ('privacy paradox'). Finally, we note that data sharing might contain yet unforeseen consequences for citizens. Ninth, technological progress ensures that a possible future profit in terms of additional knowledge from the provided data cannot be estimated at the current time ('carrier-wave principle'), while, tenth, data sharing can lead to disadvantages for other citizens ('unraveling effects').

Within the BMBF-funded project DaWID (funding reference number: 16SV8381), we want to elaborate selected areas of tension in practice. Thereby, the overall objective of DaWID is to demonstrate a data-centered, value-adding platform aiming to balance data sovereignty and data economy for both participating citizens and companies. Specifically, DaWID is addressing 'data processing', 'manipulation', 'mistrust', 'responsibility', 'anonymity', 'lock-in effects', and 'intangibility' as main areas of tension to explore practical solutions.

Integrating data sovereignty in the development of data ecosystems is at the core of our research. Future data ecosystems should follow this example and try to make data sovereignty a fundamental design principle of their business models and thus implement the European Data Strategy.

2 Introduction



Digitization has already found its way into the everyday lives of many companies and citizens. Activity trackers, smart home systems, smartphones or navigation devices have sensors and continuously record data about the user. In addition, data is generated through the use of mobility apps, online stores or simply through surfing the web. The maturity of digitization and the importance of connectivity are supported by data from the Federal Statistical Office of Germany (2020): 90% of German citizens use the internet every day or almost every day. 54% of the internet users were active in social networks and 70% made online purchases in the last three months.

It is therefore not surprising that data is considered as an asset class in its own right and that new types of data-driven business processes and value chains have emerged (World Economic Forum 2011). For companies, data marketplaces are emerging where data is securely exchanged. They allow marketplace participants to benefit from a large amount of existing personal and non-personal data (Otto et al. 2019). We believe that the importance of personal data in data ecosystems will continue to grow. A European way of linking the data economy with data sovereignty is desirable, for the welfare of companies and citizens.

> But are citizens really aware that everything around them is a kind of sensor and personal data–which is particularly worthy of protection–is constantly being generated? Do citizens have necessary control mechanisms to handle data with confidence? What are the economic, legal, and ethical implications? Do citizens know what a responsible approach of handling data looks like?

The objective of this paper is to provide insights into the interaction between data sovereignty and data economy. Citizens should be able to influence data flows of their own personal data. On the one hand, this means that citizens should be able to view, store, track and delete their data, and on the other hand, companies should create incentives for citizens to release their data. The latter can be done in monetary terms or by providing a service, but citizens will realistically not be able to gain complete control of the data generated about them (Boyd, 2012). At this point, the complicated interlocking of sovereignty and economy becomes clear, because the release of data requires a compensation that is acceptable to all parties involved.

In this paper, we highlight ten areas of tension between data sovereignty and data economics and introduce a proposition for each. To understand the implications of uniting data sovereignty and data economics, we want also to include a legal and ethical perspective. In terms of practical solutions, we want to achieve a first breakthrough with the DaWID[1] project (data-driven value creation platform for interactive, assisting service systems) funded by the German Federal Ministry of Education and Research (BMBF; funding reference number: 16SV8381). Within this project, we try to showcase how data economy approaches and data sovereignty can be successfully reconciled. Digitization is already an integral part of everyday life in our society, and we have to deal with it. The knowledge of uniting data sovereignty and data economy is the first important step in this direction.

1 www.dawid-projekt.de; *last accessed: 2021/03/26*

3

Foundations

Understanding the interplay between data sovereignty and data economics requires a set of foundations which go beyond the two topics and include additional aspects of data law and data ethics which are shortly introduced in the following.

3.1 Data Sovereignty

When talking about sovereignty in a digital context, the wording is yet to be settled, leading to several interchangeably used digital sovereignty concepts (Adonis 2019; Couture and Toupin 2019). Since these concepts share the same notion about independence, control, and autonomy (Couture and Toupin 2019), a proper distinction must answer the question: Who is the sovereign of what and where? (Aydin and Bensghir 2019)

While data sovereignty can be linked to the actual context of data use, such as at the hardware, software, and electronics level (Aydin and Bensghir 2019), the focus on 'data' implies an emphasis on data and information rather than on the underlying technological infrastructure (Couture and Toupin 2019). Thus, data sovereignty differs from (personal) technological sovereignty since ownership and self-governance of the technology itself is not necessary. With Snowden's revelations (Snowden 2019), data sovereignty became an umbrella term (Polatin-Reuben and Wright 2014). The focus shifted towards the state as data sovereign as they strive to control the data generated or passing through their national internet infrastructure. Data sovereignty became a matter of national security politics (Adonis 2019) and an attempt to extend local jurisdictions to the digital domain (Polatin-Reuben and Wright 2014). Therefore, this definition includes the actual location of the data or information.

Data sovereignty is not limited to states. Self-determination by controlling the data usage can also include organizations and individuals (Jarke et al. 2019; Zrenner et al. 2019). For organizations, exchanging, sharing, and using data enables 'data richness' and fosters business processes if done under negotiated and monitored conditions (Jarke et al. 2019).

Otherwise, companies may lose control over their data when they outsource it to the cloud, which constitutes a security risk (Henze 2020). For individuals (or society in general), data sovereignty can be interpreted as knowledge about who can access individual data and where individual data is transferred to (Posch 2017). Thus, understanding and influencing data flows is, at least with respect to their generation, intermediate transformation processes, and storage and usage (Hummel et al. 2018). Claims to power must be articulable by individuals while being enforceable by the system to ensure data sovereignty, therefore allowing individuals to be responsible for their own data.

Albeit the best mechanism to ensure data sovereignty over private data is not to share them (Filippi and McCarthy 2012). DaWID will offer solutions to (re-)establish data sovereignty for shared data for individuals and organizations.

Our understanding of data sovereignty is the ability to formulate self-defined data-usage rules, influence and trace the data/information flows while being free in the decision of (not) sharing data and migrating data whenever and wherever it is desirable.

3.2 Data Economy

The importance of data as an economic good has risen sharply in recent years, with some even calling it the "oil of the 21st century". The possibilities to collect, link, analyze and further process data in digital form open up completely new business models and enormous potential for digital value creation. This is not only borne out by the rise of internet giants like Facebook or Google, but also by the disruptive business models of Amazon, Uber and Airbnb, which have turned entire industries upside down with their platform business models (Piepenbrink 2019). Whereas in 2018, 33 zettabytes (trillion bytes) of data has been generated, this number is expected to grow to at least 175 zettabytes by 2025 (Azkan et al. 2020). Besides digitization, emerging big data technologies such as cloud computing, the Internet of Things or machine learning add to this trend (Barnaghi et al. 2013; Zhou et al. 2017).

While the steep growth of the amount of data is remarkable in itself, there is also an increased awareness for the economic value that data possesses. In fact, data has been described as "the new currency for the digital world" (Kuneva 2009). On the one hand, companies such as Facebook and Google have developed their business models around the voluntarily shared personal data of individuals, which is subsequently used to generate revenues, for instance, through ad targeting (Feijóo et al. 2014; Spiekermann and Korunovska 2017). On the other hand, third party data trading platforms have been designed in order to enable the sharing of data between different parties (Liang et al. 2018). Such trading platforms will serve as a supplier for companies that use data to improve their businesses (Glennon et al. 2020). Evidently, a new economy has been emerging over the past decades. An economy based on the exploitation of the value of data.

Although the so-called data economy can be roughly defined to include "all economic activities that utilize data" (Azkan et al. 2020), we believe that a more detailed definition is necessary and will be therefore used in the following:

> Data economy refers to the overall economic impact that data has within the context of a data ecosystem. This impact is conveyed through the generation, collection, storage, processing, distribution, analysis, elaboration, delivery, and exploitation of data.

First, this wording reflects the definition commonly used by a study for the European Commission (EC) (Glennon et al. 2020). Using a definition to include the "overall economic impact" implies that direct, indirect, and induced effects of the exchange and exploitation of data on the economy are also considered. This definition also makes it clear that a data economy is not only about collecting and storing data, but also about producing, sharing, and actually using it. This is important since data only becomes valuable with an attributed purpose. Data that is just accumulated without any purpose is of no value (Moody and Walsh 1999; Zuiderwijk et al. 2016).

Secondly, we augment the definition with the aspect of data ecosystems. A data ecosystem can be defined as a "socio-technical complex network in which actors interact and collaborate with each other to find, archive, publish, consume, or reuse data as well as to foster innovation, create value, and support new business" (S. Oliveira et al. 2019). We believe that this addition is important since it stresses the multitude of actors and their interactions constituting a data economy, rather than just focusing on the economic aspect of it. Specifically, we believe that for a data economy to be viable, aspects of data sovereignty and data ethics have to be considered for all players involved.

Finally, this adaptation of the EC's definition enables us to quantify the impact of Europe's data economy. In 2019, the EU (excl. UK) data economy generated revenues of 325 billion

thus realizing 2.6% of the total EU GDP (excl. UK). In terms of future market growth, the EU data economy is expected to grow further with a Compound Annual Growth Rate (CAGR) of 9.1% by 2025.

3.3 Data Rights

Currently, there is no ownership or other exclusive right to unembodied data. Persons and companies that are de facto owners of data sets, therefore, do not have an absolute right, that is, a right that applies to everyone, to exclude third parties from accessing or exclusively exploiting the data. The legal background is that data is not a physical object within the meaning of § 90 of the German Civil Code (BGB) and thus cannot be owned (BGH 13.10.2015, NJW 2016, 1094, Rz. 20). Rights to data therefore exist only selectively, for example, in the form of a right of the database producer to a database created by his investment according to §§ 87a ff. UrhG (Mitterer et al. 2017). Data can also be the subject of legal transactions under the law of obligations as "other objects" within the meaning of § 453 of the German Civil Code (Palandt et al. 2021). If data is traded, the data provider merely grants a de facto legal position by contract. The data recipient does not become the owner of the data due to the lack of possibility to create an absolute legal position (Paal and Hennemann 2017), but merely gains actual access to the data. In the legal literature, the question of whether or not a legal property right to data should be created continues to be controversial. It is not always clear from the contributions whether the authors are referring only to machine-generated data or also to personal data.

In the case of personal data the legal classification of it is the subject of data protection laws. The main starting point for embedding this in German law is the right to informational self-determination (BVerfGE 65, 1). This right entitles individuals to determine for themselves how their personal data is disclosed and used. As a subjective component of the fundamental right, the self-determined development and evolvement of the individual is thus protected (Roßnagel 2007). At first glance, it would appear that individuals have a kind of 'right of disposal' with regard to the data that is to be assigned to them personally, and that they can basically do with it as they please. However, this power of disposal is limited. The individual does not have a right in the sense of absolute, unrestricted control over 'its' data; rather, it is a personality that develops within the social community and is dependent on communication (BVerfGE 65, 44).

> *„Information, even if it is personal, is a reflection of social reality that cannot be attributed exclusively to the person concerned. The Geman constitution (Grundgesetz) [...] decided the dispute between individual and community in the sense of the community-relatedness and community-boundness of the person."* (BVerfGE 65, 44)

It can be inferred from this restriction that the constitution does not provide for an exclusive right to personal data. Furthermore, the GDPR excludes an exclusive right to personal data. Rather, informational self-determination was designed as a right of freedom. It thus protects freedom and not, for example, rights of disposal (Müller 2019).

Regarding machine-generated data—that is information automatically generated by a computer process, application, or other mechanism without the active intervention of a human and doesn't include any correlation with humans—proponents of a statutory data producer's right see the possibility of granting a statutory right to data to the producer of the raw data (Fezer 2017). A commercial property right to data, for example, would create an incentive to produce and market data. Although it currently appears that large quantities of data are already being produced even without such a right, a right to data could provide an incentive for new business models or improve access to or the quality of data (Wiebe 2016). In addition, such a right

could create order in the data market. This could make the market more efficient (Wiebe 2016). As a result, Ensthaler (2016) also argues in favor of this, albeit only in economic terms. Here, Ensthaler (2016) proposes the following system of allocating machine-generated data: Whoever obtains new machine-generated data from data analyses of raw data is a data producer; the owner of the source or raw data then has a claim for compensation in money according to analogy in § 951 BGB.

Most legal authors, however, argue against the creation of data ownership. For example, Kühling and Sackmann (2020) argue that the owner of (generated) data is already protected by § 202a of the German Criminal Code (StGB), at least regarding the exclusion function. In essence, the protection under criminal law of the actual control of newly generated data by § 202a of the Criminal Code („spying on data") is precisely what is often discussed under the exclusive right to data or data ownership. If it is prohibited for unauthorized persons to gain access, this presupposes an authorized person. This criminal law argument is only partially convincing, as criminal law is not primarily used to enforce civil law legal positions (von Oelffen 2020). Recently, the Brandenburg Higher Regional Court also rejected an analogous application of the provisions of the German Civil Code on the protection of ownership (OLG Brandenburg 6. November 2019, NJW-RR 2020, 54, Rz. 44). This means, the court not only considers ownership of data to be currently non-existent, but also not necessary (von Oelffen 2020).

As a result of these ongoing discussions, it is not to be expected that statutory exclusive rights to data will be created soon. Therefore, contractual regulation of rights to data is indispensable. In the case of personal data this must include the legally valid consent of the data subjects for the intended data processing. The contractual assignment of rights to data does have advantages, especially that of a flexible system that grows with technical progress (Vogt 2019).

3.4 Data Ethics

With digital transformation processes affecting almost all economic sectors, questions arise regarding the implications of data-driven business models for customers, employees, and society. In response, the still new field of data ethics has emerged. The term has not yet been uniformly defined, but Floridi and Taddeo (2016) offer an initial proposal:

> *„[D]ata ethics can be defined as the branch of ethics that studies and evaluates moral problems related to data (including generation, recording, curation, processing, dissemination, sharing and use), algorithms (including artificial intelligence [sic], artificial agents, machine learning and robots [sic]) and corresponding practices (including responsible innovation, programming, hacking and professional codes), in order to formulate and support morally good solutions (e.g. right conducts or right values).*" (Floridi and Taddeo 2016)

As a branch of applied ethics, data ethics is expected to provide practical guidance on social and policy issues. As such, data ethics is playing an increasingly important role in the data economy and, by extension, in the corporate context, where it aims to promote trust-building and appropriate use of data and algorithmic systems. Well-known data scandals in recent years, most notably the 'Facebook and Cambridge Analytica' case (Hu 2020), highlight the need to protect citizens' data sovereignty. Legal means such as the GDPR are only suitable for this purpose to a limited extent, as there may still be some room for the use of data as long as formal consent is given by users. Practices, such as the creation of user profiles without consent

('shadow profiling') (Fanta 2018), further endanger users' data sovereignty. The data ethics approach, therefore, goes beyond data protection requirements and ultimately implies self-regulation by companies instead of market-based governance.

Initial approaches for concrete measures can be observed in a series of recommendations, guidelines, principles, and questionnaires on the handling of data and AI emerging in recent years, especially, in Europe. In addition to political institutions and non-profit organizations, there is an increasing number of companies among the authors of these guidelines whose awareness of data ethics considerations seems to be growing. It can also be observed that common values such as 'autonomy', 'transparency', 'responsibility', or 'explainability' are being used as a reference for norms. The criteria for the responsible use of digital technologies are, therefore, quite clear in Europe. However, the challenge now lies in transferring these values to digital products and services. (Becker et al. 2020)

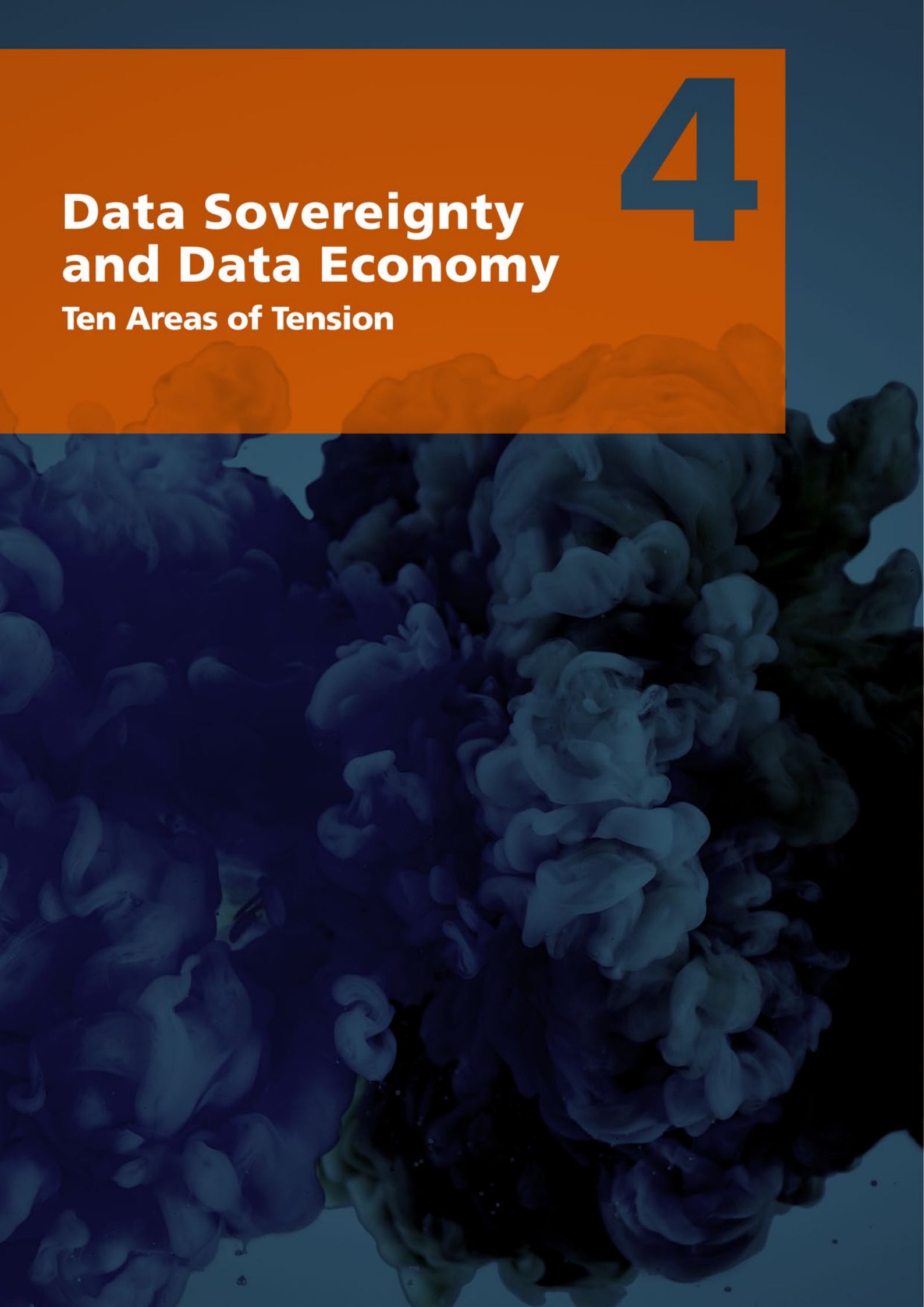
The fact that data ethics is gaining in importance in the context of data-economic developments can also be observed at the political level. For example, Denmark was the first European country to adopt a legislative amendment, adding an obligation to report on data ethics to the Danish Closing Act. Companies are required to provide justification if they cannot provide guidelines on data ethics (comply or explain principle). There are also similar considerations in Germany. For example, on October 23, 2019, the German Data Ethics Commission presented its o and made 75 recommendations for action. Among other things, it advocates the regulation of data and algorithmic systems. (German Data Ethics Commission 2019)

Time will tell how data ethics will be regulated in Germany. All in all, data ethics can make a significant contribution in the conflicting areas of data economy and data sovereignty, as it deals with the problems that arise at the interfaces of both areas.

4

Data Sovereignty and Data Economy

Ten Areas of Tension

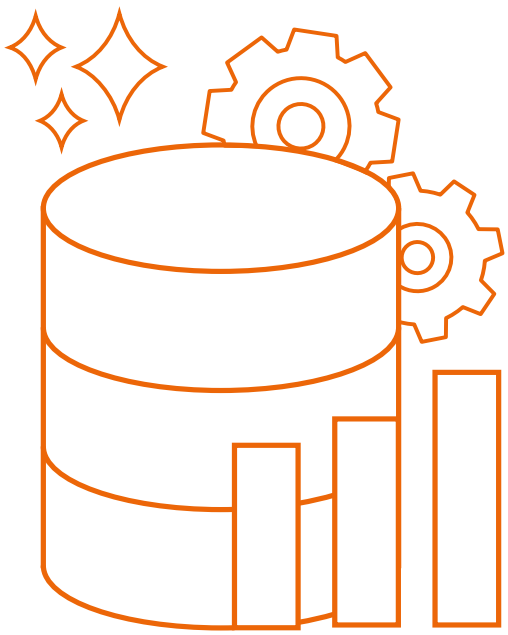


Now that the basic terms have been defined, we focus on challenges which arise when considering citizen integration into data ecosystems. We present ten areas of tension demonstrating the opportunities and risks associated with the dovetailing of data sovereignty and data economy.

4.1 Data Processing

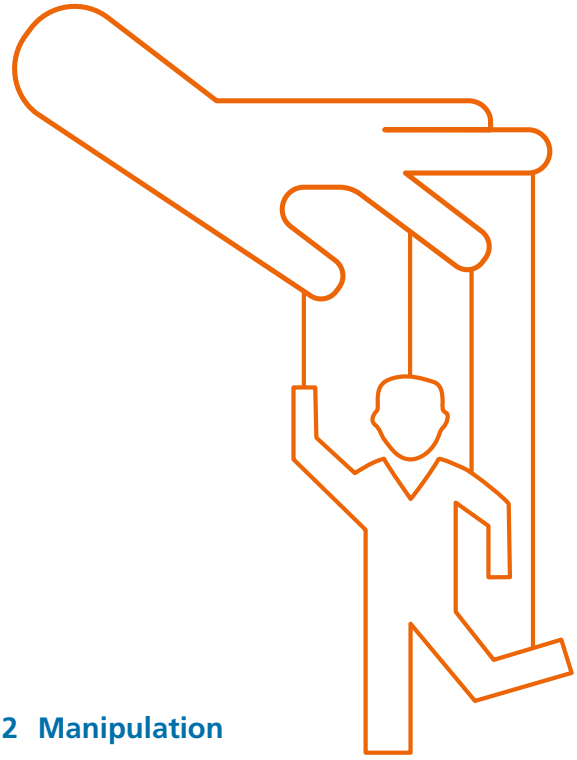
Data-based value creation is especially promising for information-intensive services and can roughly be described in the three phases data collection, information creation, and value creation (Lim et al. 2018): Given a data source, data is collected and made available (e.g., by sensors and telematics). This data is then analysed and refined to information of the data source (e.g., resource efficiency). Value is generated when this information is shared and used (e.g., by improving resource consumption).

In this process, the data of multiple sovereigns is collected and iteratively refined in phase two. These steps themselves can impose a loss of sovereignty since platform ecosystems tend to give consumers little to no insights on how they share and process their data (Sunyaev et al. 2015; Zuboff 2019). Additionally, it is unclear to what extent data sovereignty claims for the initial data sources have validity for intermediate or final data products with an increasing number of refinement steps. A change of ownership of the (intermediate) data product may occur, thus making it hard to transparently communicate where governance rights change.



Proposition #1

An individual's data sovereignty cannot be practically extended to a final data product resulting from iterative refinement steps and based on data from multiple sources. Thus, governance rights must change along the data value chain.



4.2 Manipulation

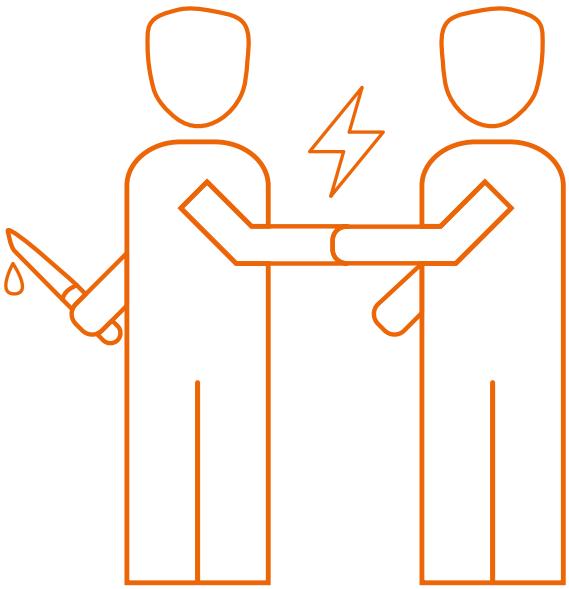
Roughly speaking, the goal of data sovereignty is establishing personal autonomy or, in other words, informational self-determination. This appears to be at odds with data-driven companies involved in data economies who are ultimately striving for profit (Zuboff 2019) and, thus, motivated to exploit opportunities for increasing profit margins. One such opportunity is manipulation of user behavior to align it with corporate objectives (Waldman 2020).

Online environments are characterized by high levels of uncertainty (Acquisti et al. 2015). (Unfortunately for citizens,) evolution favored species who are quick in adapting to environmental uncertainty (Gershman 2018). Hence, in uncertain environments, human behavior is largely guided by heuristic decision-making, which leads far quicker to 'satisficing' outcomes than rational decision-making (Simon 1956). Although heuristic decision-making proved to be evolutionary superior, knowledge of commonly used heuristics allows malicious actors (e.g., profit maximizing data-processors) to manipulate behavior (Waldman 2020); this is also often exploited in online contexts. For example, positive or negative framing of posts in online news feeds changes the emotional framing of a citizen's own posts (Kramer et al. 2014), posting a privacy notice on a website can make citizens believe that their data is better protected (Turow et al. 2018), and giving citizens more control about data sharing can make them actually disclose more sensitive information (Brandimarte et al. 2012).

The list of identified heuristics (cognitive biases, in terms of Kahneman and Tversky (1974)) applied by users is already long (Arnott 2006), but probably incomplete. Obvious heuristics that can be exploited by malicious actors for manipulation of user behavior in data economies are, for instance, control bias (e.g., give citizens control over unprofitable information flows to increase overall data sharing), completeness bias (e.g., provide citizens with a lot of information so that they do not realize that unfavorable information practices are omitted), or desirability bias (e.g., stress the benefits of data sharing and downplay the risks) (Arnott 2006). Up until now, research has only scratched the surface of how heuristics are exploited by online companies (Acquisti et al. 2020) and it remains questionable whether all avenues for manipulation of user behavior in data markets can be controlled. Hence, without rapid and fierce enforcement of manipulation bans and high levels of corporate social responsibility (Martin 2016), data economies will obliterate data sovereignty since there is no personal autonomy under conditions of behavioral manipulation.

Proposition #2

Without carefully designed codes of conduct that are rapidly and fiercely enforced, data economies are predominantly a powerful tool for consumer manipulation.



4.3 Mistrust

In early 2018, the disclosure of 50 million data records of Facebook users to the data analytics company Cambridge Analytica caused a global scandal (Cadwalladr and Graham-Harrison 2018). It was not the first data scandal of this size; however, it revealed a fundamental problem with the handling of data and transparency in the data economy. Facebook had known about the data transfer since 2015, but kept quiet about the issue until 2018, only taking a stand on the incident in response to public pressure. Cases like this contribute to citizens being distrustful of companies regarding their data and more cautious about sharing personal information (Rantanen 2019). However, the core of the data economy is based on as many citizens as possible being willing to share their data. In the area of conflict between data economy and data sovereignty, mistrust therefore becomes a major challenge for companies when data-sovereign citizens can view, store, influence, track, and delete their data at any time.

To strengthen citizens' trust in the data economy, it should be clearly communicated how data sovereignty is ensured on digital platforms. For this, companies need reliable control mechanisms that not only implement the legally required data protection, but also support the implementation of data sovereignty through concrete measures. Among other things, promoting transparency, traceability and digital literacy among citizens can contribute here. It is crucial that these measures have a tangible impact on the use of the platform.

Proposition #3

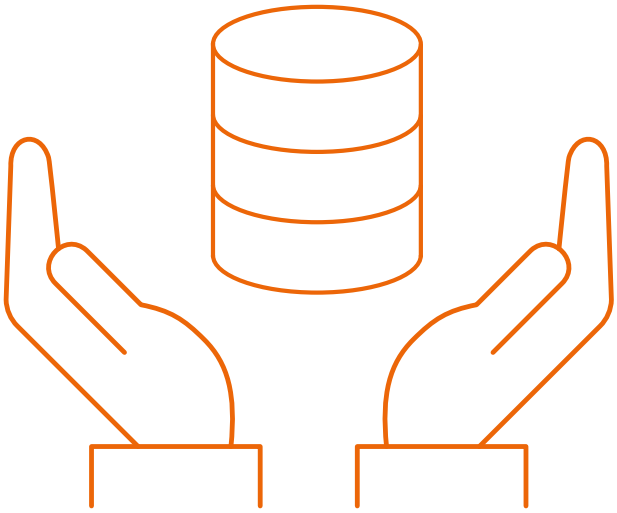
Trust in a data economy must be earned, not claimed by companies.

4.4 Responsibility

In the area of conflict between data economy and data sovereignty, the question of responsibility for data arises. Who is responsible for data storage and use in a platform ecosystem with (data-)sovereign participants?

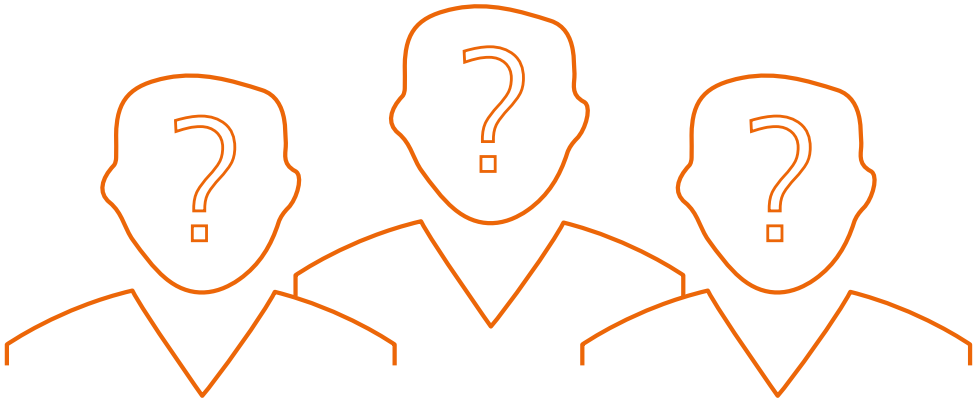
From the principle of data sovereignty, one can initially assume an attribution to the citizen. After all, if citizens are sovereigns over their data and can, thus, influence which data they make available to which company and whether they participate in business processes, then a certain degree of responsibility for the data follows. If data sovereignty was fully guaranteed, no one would be forced to transfer their data to a particular company. There would always be the option of deleting the data or otherwise taking influence. However, it would require a permanent preoccupation with and monitoring of all the data that a citizen has passed on in the context of the data economy. Without sufficient knowledge of how data is processed in data value chains, it is almost impossible to fulfill such responsibilities. So far, it is difficult to understand from an external perspective what exactly the internal processes of data-driven companies look like.

It is therefore the responsibility of companies as operators and developers of data-driven platforms to create sufficient transparency and to educate citizens about the data value chains in question. Moreover, a company is responsible for the data it holds on behalf of a data-sovereign citizen, as the citizen has no influence on the processes and security measures in the company. The crucial question, therefore, is not who is responsible, but who takes responsibility.



Proposition #4

In a data economy, companies cannot build business models without also considering issues of digital responsibility.



4.5 Anonymity

From a technical perspective, anonymity is achieved whenever a particular subject cannot be identified within a set of more than one subjects (Pfitzmann and Köhntopp 2001) and is a requirement when dealing with sensitive information (e.g., health records of patients (Dehling and Sunyaev 2014)). If a subject can only be mapped to an identifier (e.g., 'subject #42') anonymity is violated but pseudonymity is still achieved. In a data ecosystem, anonymization may be a requirement for data processing and storing, thus complicating data provenance tracking and subject remuneration. Whenever subsets of data are extracted out of an anonymized collection, the tracing of data becomes convoluted. Sender anonymity and relationship anonymity (Pfitzmann and Köhntopp 2001) may be undesired for data ecosystems since linkability between sender and message (data) may be necessary to claim data sovereignty. Therefore, weaker concepts, such as pseudonymity, may be considered to implement data sovereignty.

Proposition #5

Data sovereignty cannot be achieved without relaxing anonymity assumptions (e.g., falling back to pseudonymity).

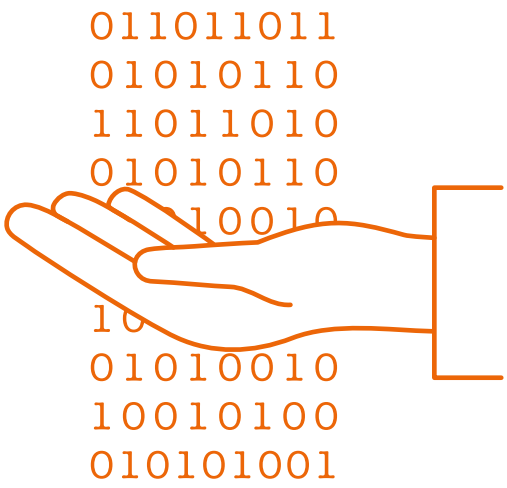
4.6 Lock-In Effects

Marketeers describe lock-in effects as users being unwilling or unable to switch services or products due to high costs associated with switching (Liebowitz and Margolis 1994). This effect is commonly observed in digitized services due to three reasons (Shapiro and Varian 1998): First, users are often less likely to change services with a growing number of users. This is because the value of many information technologies depends on the number of users. Secondly, switching costs are also high because it often implies the value of the data shared over time is at risk of being lost. This is because the value of a service also increases as more data is shared with the service provider. However, service providers often offer only low interoperability for data exchange with other providers resulting in a lock-in effect (Filippi and McCarthy 2012). Third, this becomes even more pronounced when several distinct services of the same provider are being used (i.e., a centralization of services to a single provider takes place). Through combining the data shared across services, the value delivered but also the accompanying lock-in increases even further (Moody and Walsh 1999).

The prevailing lock-in effect in digitized services negatively affects both data sovereignty and data economy (Filippi and McCarthy 2012). Data sovereignty is impaired because even if users might feel their privacy needs are not met with their current provider, they will not change providers due to high switching costs. Data economy is negatively affected because competition on the market is lowered. A high user concentration at few players with high switching costs is characteristic of monopoly building-mechanisms and high entry barriers for new players. In order to surmount lock-in effects, data portability between platforms should be increased (ideally, without too much regulation (Demary 2015)). If users can easily transfer their data from one platform to another, switching costs are significantly lowered (Swire and Lagos 2013).

Proposition #6

A viable data-sharing ecosystem is suitable to lower users' switching cost by increasing availability, transparency, and mobility of data across actors.



4.7 Intangibility

Data cannot have the corporality of objects within the meaning of § 90 of the German Civil Code because, unlike corporal objects, they are characterized by their non-rivalry, non-exclusivity and inexhaustibility, i.e., they can be used by numerous users without impairing each other's use, can be copied at will without any particular financial expense and are not subject to wear and tear or aging (OLG Brandenburg November 6, 2019, NJW-RR 2020, 54, para. 44). However, even if data is not subject to wear and tear or aging the pure value of the data itself depends on its age. Usually, data loses in value as more outdated it becomes.

Undoubtedly, however, data is valuable as can be seen from the market capitalization of companies such as Amazon, Google, Facebook, and the like. And there is no doubt that this capital is generated on the basis of user data without them adequately participating in the value creation.

This raises the question of why old concepts should be allowed to persist in a world that has been changed primarily by digitization. What is to be said against developing the law further that there can also be a property right to data? On this assumption that not only copyright law but also data law gives rise to property in the sense of Article 14 of the German Constitution (Grundgesetz), a new data law system could be designed that creates a data right in the sense of a sui generis immaterial property right (Riechert 2019).

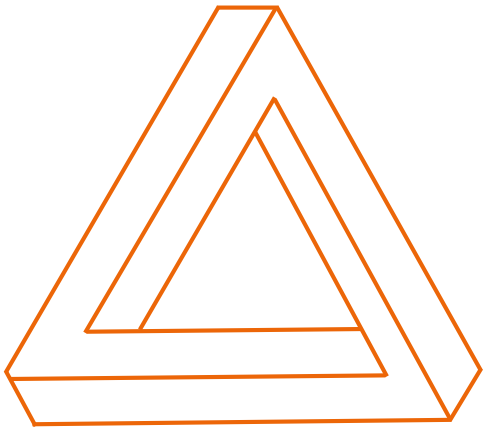
Proposition #7

When today's legal systems were created, data did not yet play such a decisive role as a valuable, intangible asset. However, data and its continuously rising value must be taken into consideration by lawmakers to stay abreast of that change.

4.8 Privacy Paradox

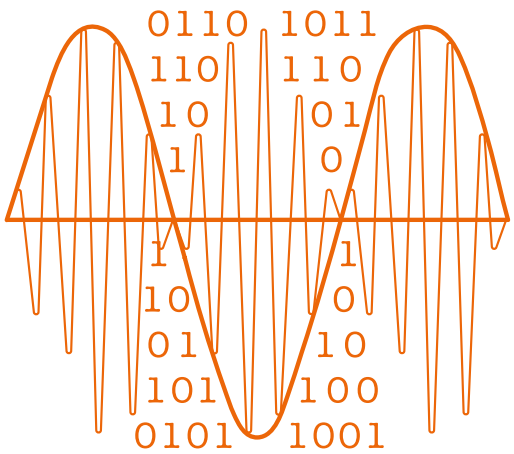
We shop online and use social media thus consciously or unconsciously sharing a variety of personal data—and complain at the same time about a lack of data protection. This contradiction between carefree behavior on the one hand and worries about a lack of privacy on the other is the so-called privacy paradox (Engels and Grunewald 2017).

In the literature, there are four main approaches to explain the phenomenon (Barth and Jong 2017). Rational approaches assume that users assess and weigh the benefits and risks of sharing their data (Culnan and Armstrong 1999; Simon 1955). As a result, the paradox can be explained by benefits (e.g., networking with friends) outweighing the risks (e.g., exploitation of data shared, data theft). The vast majority of research assumes, however, that irrationality plays a significant role in the decision-making process of sharing or not sharing data. Therefore, a second line of theories include various cognitive biases in the assumed risk-benefit calculation of users (Acquisti and Grossklags 2005; Simon 1997). For example, it has been shown, that users adapt simplified mental models, so-called heuristics, that systematically favor benefits (Pötzsch 2010). This is because even if theoretically all privacy-related information would be available, a lot of cognitive effort would be required to process and weigh this information rationally. Heuristics are a shortcut in decision-making that spare cognitive resources. A third approach assumes that citizens are prevented to align their privacy behavior with their privacy attitude because of a lack of information provided by internet providers (Meynhardt 2009). Lastly, a fourth approach challenges the conception of the privacy paradox per se (Martin 2020; Solove 2020). Here it is argued that the privacy paradox fails to recognize that privacy-related behavior is highly context-dependent and influenced by multiple factors. The notion of a paradox is misleading, as broader attitudes by definition cannot be perfectly aligned with context-specific behavior.



Proposition #8

Simply informing and sensitizing citizens falls short of effective privacy management. In order to improve privacy-related decision-making, privacy-related heuristics and biases must be reflected in the user interface design.



4.9 Carrier-Wave Principle

In communication technology, a carrier wave is set up with a certain frequency (or frequencies) modulated with a signal to transmit encoded data. Sinnreich and Gilbert (2019) propose the theoretical premise that every cultural artifact acts as a carrier wave transmitting multiple layers of information intentionally or unintentionally embedded into the artifact by its creator. Emerging technologies allow for derivation of new information from an artifact that is interpreted under a given social or instructional context. For instance, genomics research is transferred to cloud computing due to storage and computational benefits—the genome and the corresponding metadata act as artifacts in the new context of cloud computing. Since genomes carry information about individuals and their relatives, it is necessary to build genomic cloud platforms that benefit healthcare research without imposing information security and privacy risks (Thiebes et al. 2016).

In the context of data sovereignty, this means that it is unpredictable what information can be extracted from data in the future. For instance, a new machine learning algorithm based on vast social media data could determine an individual's ideology based on mere metadata. While the default deletion of data after a given timespan can serve as a mechanism to reduce the windows of exhibition of a particular dataset, all copies or data products derived from this data set remain unchanged and can act as a carrier wave.

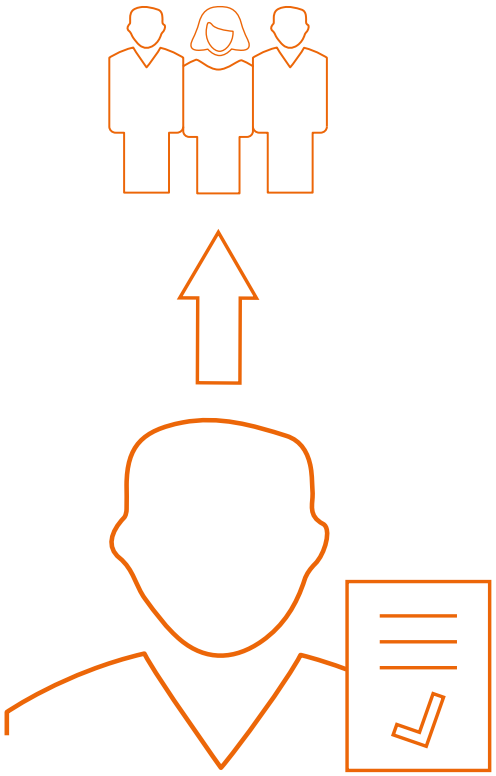
Proposition #9

Technological and cultural developments are unpredictable. Data shared today could reveal more information than initially intended, leading to consumer regret about past sharing decisions.

4.10 Unraveling Effects

The data sovereignty of one platform participant can have implications for the data sovereignty of other participants (Hummel et al. 2018). So-called unraveling effects motivate "… self-interested actors to fully disclose their personal information for economic gain" (Peppet 2011). For instance, unraveling disclosure of health data to an insurance company for the exchange of lower monthly payment dues. This can lead to challenges since information about consumers who restrict their data sharing can be learned from the data shared by other consumers (Peppet 2011).

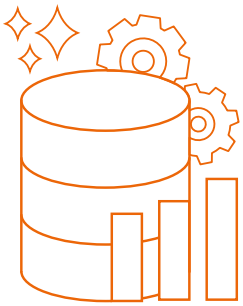
The dilemma is that one participant's data sovereignty (voluntary data sharing) negatively affects other participants' data sovereignty by either revealing their information or compelling them to share their data too. Since not sending a signal is often interpreted as bad sign and is associated with low 'quality' expectations of the data (Peppet, 2011). Thus, data sovereignty also implies a responsibility for others. From a data economy perspective, this makes it challenging to discern whether consumers should actually be allowed to give data they have away and whether they need to obtain consent from and offer compensation to other consumers that could be potentially affected by the sharing of data (Humbert et al. 2019).



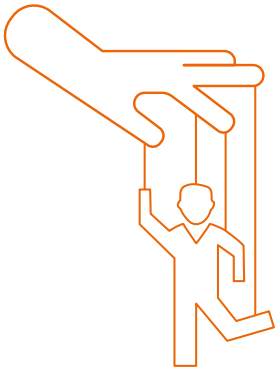
Proposition #10

A platform ecosystem that includes incentive mechanisms for sharing data will lead to unraveling effects that will only benefit a few participants while being disadvantageous for others, thus leading to a collision of an individuals' data sovereignty with the interests of other sovereigns.

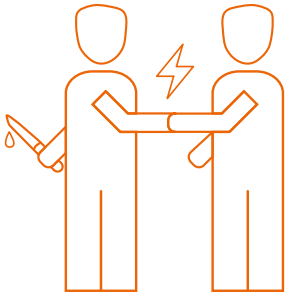
Overview: Ten areas of tension



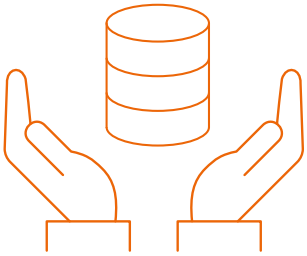
Data Processing



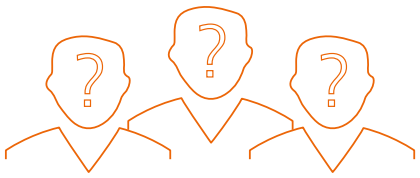
Manipulation



Mistrust

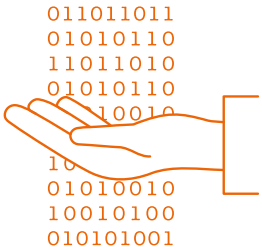


Responsibility

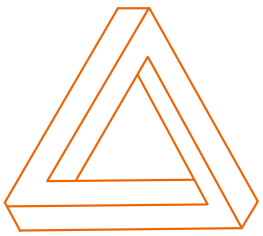


Anonymity

Lock-In Effects

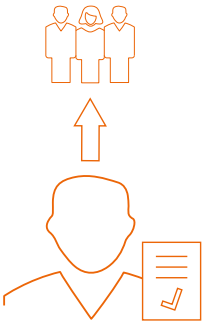


Intangibility



Privacy Paradox

Carrier-Wave Principle



Unraveling Effects

5

Application in Practice and Outlook

As outlined in the previous chapter, we state that a multitude of propositions have to be considered in order to catenate the domains and principles of data sovereignty and data economy. The following section finally outlines how we recommend to set up current research to develop solutions addressing those specific propositions.

To date, citizens have limited opportunities to exercise data sovereignty in data ecosystems. Data ecosystems are often platforms where only organizations or companies can participate while individuals are commonly neglected (Nachira et al. 2007; Otto et al. 2019; Tiwana 2013). One of the reasons is the fact that data from or about citizens is usually personal data and thus requires more sensitive treatment (Spiekermann et al. 2015). Therefore, business processes handling such data must fulfill certain characteristics as they must be GDPR-compliant (European Parliament and Council of European Union 2016). Citizens' awareness about their data is not yet sufficiently sensitized, however, so that they don't know the value of their own data (Acquisti et al. 2013). Nevertheless, the interest of citizens, companies, or states in being able to make sovereign decisions concerning their own data and their desire to benefit from data sharing are rising (Benndorf and Normann 2018; Spiekermann et al. 2015). To enable an informational self-determined life for every citizen and to demonstrate which disciplines are crucial for citizens' data sovereignty, Fraunhofer ISST developed the so-called Digital Life Journey[2] (DLJ; Meister and Otto (2019)). This framework includes considerations of society, technology, ethics, law, and economics. More precisely, to describe the maturity level of transparency and control of one's own data, the DLJ defines three stages of development: the digital shadow, the digital me, and the digital twin. The DLJ framework considers the digital me as a first evolutionary step desirable for citizens as it represents a holistic image of the citizens' data available in data ecosystems and thus allows for insights into their personal data being stored.

A first project embedded in the context of the DLJ is DaWID. DaWID stands for „data-driven value creation platform for interactive, assisting service systems" and is funded by the German Federal Ministry of Education and Research (BMBF; funding number: 16SV8381). The consortium consists of the project partners Fraunhofer Institute for Software and Systems Engineering ISST, Fraunhofer Center for International Management and Knowledge Economy IMW, the Deutsche Telekom AG, the Institute for Digital Transformation in Healthcare GmbH (idigiT), and the Critical Information Infrastructures (cii) research group at the Institute of Applied Informatics and Formal Description Methods (AIFB) of the Karlsruhe Institute of Technology (KIT). The project runs from 01.02.2020 to 31.01.2023 and the project management organisation is VDI/VDE Innovation + Technology GmbH[3].

The project objective is to investigate, develop, and test a data-centered value-added platform aiming at balancing data sovereignty and data economy for all players involved. On the one hand, data flows should be transparent and data use should be comprehensible. On the other hand, from a data economy perspective, novel cooperation and business models should be enabled to achieve 'data refinement' as the goal of digital value-added processes. The project does not create a new, singular platform, but rather develops a cross-platform mechanism for linking solutions of data sovereignty to a holistic data ecosystem while particularly considering citizens as data sources. Using concrete use cases ('smart urban mobility' and 'smart home with activity trackers'), the consortium intends to empower citizens with the opportunity to make sovereign decisions about their data and to participate in business models which are based on their personal data. The solutions aim to combine data sovereignty and data economy fairly for both

2 *www.digitallifejourney.de/en; last accessed: 2021/03/26*

3 *www.vdivde-it.de/en; last accessed: 2021/03/26*

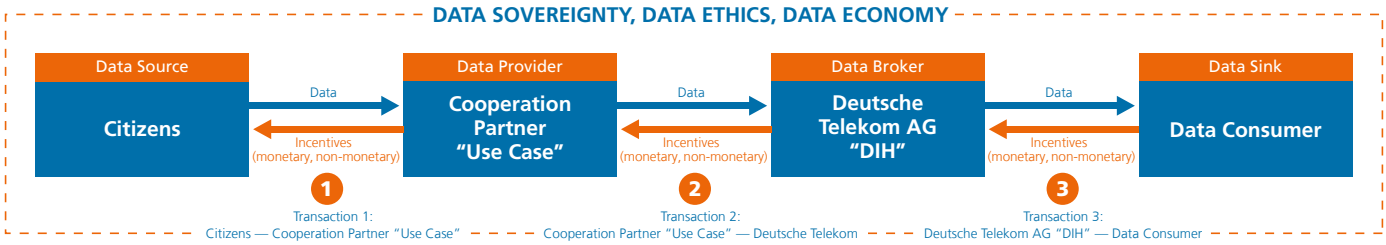


Figure 1

citizens and companies. For this purpose, a framework of 'data and incentives flows' as illustrated in Figure 1 was developed. Thereby, four actors were proposed, which are interrelated and form a value chain. In the first place there is the data source, which is embodied by the citizen. The source provides its data to a data provider by using the services of a cooperation partner (transaction 1). In return, it receives monetary or non-monetary compensation. Subsequently, the data provider establishes a relationship with the data broker in the form of the Data Intelligence Hub (DIH) of the Deutsche Telekom AG (transaction 2). The citizens can initially decide whether they want to make their data available to the DIH or whether they rather reject. The DIH refers to a data marketplace as the framework's first architectural component that is required to fulfill the high security criteria set by the International Data Spaces Association[4] in order to enable the development of data analysis tools and algorithms. The last link in the value chain is the data sink, which represents the data consumer. This actor obtains the data from the DIH and thus commits itself to defined data usage rules. The consumer can use the acquired data to unlock new business areas and consequently enter new markets. Product or service enhancements are possible under consideration in the terms of use.

Ensuring data sovereignty in profit-maximizing data economies contains several challenges. Consequently, it might not appeal economical for a company to empower citizens to control their data flows. Nevertheless, in order to strengthen the sovereignty of the citizen, our objective is to develop concepts that bring together the interests of both citizens and companies. Within DaWID, we aim at evaluating a subset of our areas of tension in practice. The project includes several main themes such as data sovereignty, information flow management, business models, and data ethics. For instance, we examine 'data processing', 'manipulation', and 'anonymity' in the context of data sovereignty and information flow management. We want to ensure safe data transfers while considering aspects of data sovereignty with policy definition languages, data use and access concepts, as well as data ecosystems technologies such as International Data Spaces. Business models address the areas 'lock-in effects' and 'intangibility'. Concepts for explicit data business models, digital contracts, and pricing of data are in the focus. The areas 'mistrust' and 'responsibility' can be allocated to data ethics developing measures for a "data ethics by design". To apply all these selected areas of tension in practice, we want to embed our solutions in an existing data ecosystem (e.g., DIH). The last remaining three areas 'privacy paradox', 'carrier-wave principle', and 'unraveling effects' are not part of our detailed consideration. We want to call on other research groups to explore these areas.

All in all, our areas of tension emphasize that it is possible to balance data sovereignty and data economics. The union of these two powerful domains brings up a variety of challenges that future solutions must balance or resolve. It is our aim to verify a selection of our propositions in practice within the BMBF-funded project DaWID, to find practical implementations for best practices and thus contribute to a further development of (European) data spaces.

4 *www.internationaldataspaces.org; last accessed: 2021/03/26*

6

References

Acquisti, A., Brandimarte, L., and Loewenstein, G. 2015. "Privacy and human behavior in the age of information," *Science* (347:6221), pp. 509-514 (doi: 10.1126/science.aaa1465).

Acquisti, A., Brandimarte, L., and Loewenstein, G. 2020. "Secrets and Likes: The Drive for Privacy and the Difficulty of Achieving It in the Digital Age," *Journal of Consumer Psychology* (30:4), pp. 736-758 (doi: 10.1002/jcpy.1191).

Acquisti, A., and Grossklags, J. 2005. "Privacy and rationality in individual decision making," *IEEE Security and Privacy Magazine* (3:1), pp. 26-33 (doi: 10.1109/msp.2005.22).

Acquisti, A., John, L. K., and Loewenstein, G. 2013. "What Is Privacy Worth?" *The Journal of Legal Studies* (42:2), pp. 249-274 (doi: 10.1086/671754).

Adonis, A. A. 2019. "Critical Engagement on Digital Sovereignty in International Relations: Actor Transformation and Global Hierarchy," *Global: Jurnal Politik Internasional* (21:2), pp. 262-282 (doi: 10.7454/global.v21i2.412).

Arnott, D. 2006. "Cognitive biases and decision support systems development: a design science approach," *Information Systems Journal* (16:1), pp. 55-78 (doi: 10.1111/j.1365-2575.2006.00208.x).

Aydin, A., and Bensghir, T. K. 2019. "Digital Data Sovereignty: Towards a Conceptual Framework," *2019 1st International Informatics and Software Engineering Conference (UBMYK)* (doi: 10.1109/UBMYK48245.2019.8965469).

Azkan, C., Goecke, H., and Spiekermann, M. 2020. "Forschungsbereiche der Datenökonomie," *Wirtschaftsdienst* (100:2), pp. 124-127 (doi: 10.1007/s10273-020-2582-x).

Barnaghi, P., Sheth, A., and Henson, C. 2013. "From Data to Actionable Knowledge: Big Data Challenges in the Web of Things," *IEEE Intelligent Systems* (28:6), pp. 6-11 (doi: 10.1109/mis.2013.142).

Barth, S., and Jong, M. D.T. de 2017. "The privacy paradox – Investigating discrepancies between expressed privacy concerns and actual online behavior – A systematic literature review," *Telematics and Informatics* (34:7), pp. 1038-1058 (doi: 10.1016/j.tele.2017.04.013).

Becker, S. J., Nemat, A. T., and Rebbert, M. 2020. "Der Ruf nach operationalisierbarer Ethik – Unternehmensverantwortung in der digitalen Welt," in *Unternehmensverantwortung im digitalen Wandel*: *Ein Debattenbeitrag zu Corporate Digital Responsibility*, Bertelsmann Stiftung and Wittenberg-Zentrum für Globale Ethik (eds.), pp. 28-34.

Benndorf, V., and Normann, H.-T. 2018. "The Willingness to Sell Personal Data," *The Scandinavian Journal of Economics* (120:4), pp. 1260-1278 (doi: 10.1111/sjoe.12247).

Brandimarte, L., Acquisti, A., and Loewenstein, G. 2012. "Misplaced Confidences: Privacy and the Control Paradox," *Social Psychological and Personality Science* (4:3), pp. 340-347 (doi: 10.1177/1948550612455931).

Cadwalladr, C., and Graham-Harrison, E. 2018. *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Accessed 29 April 2021.

Couture, S., and Toupin, S. 2019. "What does the notion of "sovereignty" mean when referring to the digital?" *New Media & Society* (21:10), pp. 2305-2322 (doi: 10.1177/1461444819865984).

Culnan, M. J., and Armstrong, P. K. 1999. "Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation," *Organization Science* (10:1), pp. 104-115 (doi: 10.1287/orsc.10.1.104).

Dehling, T., and Sunyaev, A. 2014. "Secure provision of patient-centered health information technology services in public networks-leveraging security and privacy features provided by the German nationwide health information technology infrastructure," *Electronic Markets* (24:2), pp. 89-99 (doi: 10.1007/s12525-013-0150-6).

Demary, V. 2015. "The platformization of digital markets: Comments on the public consultation of the European Commission on the regulatory environment for platforms, online intermediaries, data and cloud computing and the collaborative economy," *IW Policy Papers* 39/2015, Köln: Institut der deutschen Wirtschaft (IW).

Engels, B., and Grunewald, M. 2017. "Das Privacy Paradox: Digitalisierung versus Privatsphäre," 57.2017, Institut der deutschen Wirtschaft (IW) / German Economic Institute.

Ensthaler, J. 2016. "Industrie 4.0 und die Berechtigung an Daten," *NJW*, pp. 3473-3478.

European Parliament and Council of European Union 2016. *Regulation (EU) 2016/679.* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC. Accessed 29 April 2021.

Fanta, A. 2018. *Ob Nutzer oder nicht: Facebook legt Schattenprofile über alle an.* https://netzpolitik.org/2018/ob-nutzer-oder-nicht-facebook-legt-schattenprofile-ueber-alle-an. Accessed 29 April 2021.

Federal Government 2021. *Datenstrategie der Bundesregierung: Eine Innovationsstrategie für gesellschaftlichen Fortschritt und nachhaltiges Wachstum.* https://www.bundesregierung.de/breg-de/suche/datenstrategie-der-bundesregierung-1845632. Accessed 22 February 2021.

Federal Statistical Office of Germany (Destatis) 2020. *Private Haushalte in der Informationsgesellschaft - Nutzung von Informations- und Kommunikationstechnologien: Fachserie 15 Reihe 4 - 2019.* https://www.destatis.de/DE/Themen/Gesellschaft-Umwelt/Einkommen-Konsum-Lebensbedingungen/IT-Nutzung/Publikationen/Downloads-IT-Nutzung/private-haushalte-ikt-2150400197004.pdf?__blob=publicationFile. Accessed 29 April 2021.

Feijóo, C., Gómez-Barroso, J. L., and Voigt, P. 2014. "Exploring the economic value of personal information from firms' financial statements," *International Journal of Information Management* (34:2), pp. 248-256 (doi: 10.1016/j.ijinfomgt.2013.12.005).

Fezer, K.-H. 2017. "Dateneigentum der Bürger," ZD (7:3), pp. 99-105.

Filippi, P. de, and McCarthy, S. 2012. "Cloud Computing: Centralization and Data Sovereignty," *European Journal of Law and Technology* (3:2).

Floridi, L., and Taddeo, M. 2016. "What is data ethics?" *Philosophical transactions. Series A, Mathematical, physical, and engineering sciences* (374:2083) (doi: 10.1098/rsta.2016.0360).

German Data Ethics Commission 2019. *Opinion of the Data Ethics Commission.* https://datenethikkommission.de/wp-content/uploads/DEK_Gutachten_engl_bf_200121.pdf. Accessed 29 April 2021.

Gershman, S. J. 2018. "Deconstructing the human algorithms for exploration," *Cognition* (173), pp. 34-42 (doi: 10.1016/j.cognition.2017.12.014}).

Glennon, M., La Croce, C., Cattaneo, G., Micheletti, G., and Mitta, C. 2020. *The European data market monitoring tool: Key facts & figures, first policy conclusions, data landscape and quantified stories: d2.9 final study report.* https://op.europa.eu/en/publication-detail/-/publication/9fb0599f-c18f-11ea-b3a4-01aa75ed71a1/language-en.

Henze, M. 2020. "The Quest for Secure and Privacy-preserving Cloud-based Industrial Cooperation," *IEEE Conference on Communications and Network Security (CNS)*, pp. 1-5 (doi: 10.1109/CNS48642.2020.9162199).

Hu, M. 2020. "Cambridge Analytica's black box," *Big Data & Society* (7:2) (doi: 10.1177/2053951720938091).

Humbert, M., Trubert, B., and Huguenin, K. 2019. "A Survey on Interdependent Privacy," *ACM Comput. Surv.* (52:6) (doi: 10.1145/3360498).

Hummel, P., Braun, M., Augsberg, S., and Dabrock, P. 2018. "Sovereignty And Data Sharing," *ITU Journal: ICT Discoveries (25:08).*

Jarke, M., Otto, B., and Ram, S. 2019. "Data Sovereignty and Data Space Ecosystems," *Business & Information Systems Engineering* (61:5), pp. 549-550 (doi: 10.1007/s12599-019-00614-2).

Kramer, A. D. I., Guillory, J. E., and Hancock, J. T. 2014. "Experimental evidence of massive-scale emotional contagion through social networks," *Proceedings of the National Academy of Sciences of the United States of America* (111:24), pp. 8788-8790 (doi: 10.1073/pnas.1320040111}).

Kühling, J., and Sackmann, F. 2020. "Irrweg "Dateneigentum"," ZD (10:1), pp. 24-30.

Kuneva, M. 2009. *Roundtable on online data collection, targeting and profiling*. Keynote Speech. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156. Accessed 29 April 2021.

Liang, F., Yu, W., An, D., Yang, Q., Fu, X., and Zhao, W. 2018. "A Survey on Big Data Market: Pricing, Trading and Protection," *IEEE Access* (6), pp. 15132-15154 (doi: 10.1109/access.2018.2806881).

Liebowitz, S. J., and Margolis, S. E. 1994. "Network Externality: An Uncommon Tragedy," *Journal of Economic Perspectives* (8:2), pp. 133-150 (doi: 10.1257/jep.8.2.133).

Lim, C., Kim, K.-H., Kim, M.-J., Heo, J.-Y., Kim, K.-J., and Maglio, P. P. 2018. "From data to value: A nine-factor framework for data-based value creation in information-intensive services," *International Journal of Information Management* (39), pp. 121-135 (doi: 10.1016/j.ijinfomgt.2017.12.007).

Martin, K. 2020. "Breaking the Privacy Paradox: The Value of Privacy and Associated Duty of Firms," *Business Ethics Quarterly* (30:1), pp. 65-96 (doi: 10.1017/beq.2019.24).

Martin, K. D. 2016. "Understanding privacy online: Development of a social contract approach to privacy," *Journal of Business Ethics* (137:3), pp. 551-569 (doi: 10.1007/s10551-015-2565-9).

Meister, S., and Otto, B. 2019. "Digital Life Journey: Framework for a self-determined life of citizens in an increasingly digitized world (basic research paper)," Fraunhofer Institute for Software and Systems Engineering ISST, B. Otto and J. Rehof (eds.), Dortmund.

Meynhardt, T. 2009. "Public Value Inside: What is Public Value Creation?" *International Journal of Public Administration* (32:3-4), pp. 192-219 (doi: 10.1080/01900690902732632).

Mitterer, K., Wiedemann M., and Zwissler, T. 2017. *BB-Gesetzgebungs- und Rechtsprechungsreport zu Industrie 4.0 und Digitalisierung*.

Moody, D. L., and Walsh, P. 1999. "Measuring the Value Of Information - An Asset Valuation Approach," in *European Conference on Information Systems*, pp. 496-512.

Müller, J. K. M. 2019. "Dateneigentum in der vierten industriellen Revolution?" *Datenschutz Datensicherheit* (43:3), pp. 159-166 (doi: 10.1007/s11623-019-1084-8).

Nachira, F., Nicolai, A., and Dini, P. 2007. *Digital business ecosystems*, Luxembourg: Publications Office.

Opher, A., Chou, A., Onda, A., and Sounderrajan, K. 2016. *The Rise of the Data Economy: Driving Value through Internet of Things Data Monetization*: *A Perspective for Chief Digital Officers and Chief Technology Officers*. https://www.ibm.com/downloads/cas/4JROLDQ7. Accessed 29 April 2021.

Otto, B., Cirullies, J., Opriel, S., Holtkamp, B., Howar, F., Jürjens, J., Lis, D., Meister, S., Möller, F., Pettenpohl, H., and Spiekermann, M. 2019. "Data Ecosystems: Conceptual Foundations, Constituents and Recommendations for Action," Fraunhofer Institute for Software and Systems Engineering ISST, Dortmund.

Paal, B., and Hennemann, M. 2017. "Big Data im Recht – Wettbewerbs- und daten(schutz)rechtliche Herausforderungen," *NJW* (70:24), pp. 1697-1701.

Palandt, O., Ellenberger, J., Götz, I., Grüneberg, C., and Herrler, S. 2021. *Bürgerliches Gesetzbuch*: *Mit Nebengesetzen insbesondere mit Einführungsgesetz (Auszug) einschließlich Rom I-, Rom II und Rom III-Verordnungen sowie EU-Güterrechtsverordnungen, Haager Unterhaltsprotokoll und EU-Erbrechtsverordnung, Allgemeines Gleichbehandlungsgesetz (Auszug), Wohn- und Betreuungsvertragsgesetz, Unterlassungsklagengesetz (PalHome), Produkthaftungsgesetz, Erbbaurechtsgesetz, Wohnungseigentumsgesetz, Versorgungsausgleichsgesetz, Lebenspartnerschaftsgesetz (PalHome), Gewaltschutzgesetz*, München: C.H.Beck.

Peppet, S. R. 2011. "Unraveling privacy: The personal prospectus and the threat of a full-disclosure future," *Nw. UL Rev.* (105), p. 1153.

Pfitzmann, A., and Köhntopp, M. 2001. "Anonymity, Unobservability, and Pseudonymity — A Proposal for Terminology," in *Designing Privacy Enhancing Technologies*, H. Federrath (ed.), Berlin, Heidelberg: Springer, pp. 1-9.

Piepenbrink, J. 2019. "Datenökonomie," *Aus Politik und Zeitgeschichte* (69:24-26).

Polatin-Reuben, D., and Wright, J. 2014. "An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet," in *4th USENIX Workshop on Free and Open Communications on the Internet (FOCI 14)*, San Diego, California, USA: USENIX Association.

Posch, R. 2017. "Digital sovereignty and IT-security for a prosperous society," in *Informatics in the Future*, H. Werthner and F. van Harmelen (eds.), Cham, CH: Springer, pp. 77-86.

Pötzsch, S. 2010. "Privacy-Awareness Information for Web Forums: Results from an Empirical Study," in *Proceedings of the 6th Nordic Conference on Human-Computer Interaction*: *Extending Boundaries*, E. T. Hvannberg (ed.), New York, NY: ACM, pp. 363-372.

Rantanen, M. M. 2019. "Towards Ethical Guidelines for Fair Data Economy – Thematic Analysis of Values of Europeans," in *Proceedings of the Third Seminar on Technology Ethics*, CEUR Workshop Proceedings, pp. 27-38.

Riechert, A. 2019. "Dateneigentum - ein unauflösbarer Interessenkonflikt?" *Datenschutz und Datensicherheit* (43:6), pp. 353-360 (doi: 10.1007/s11623-019-1121-7).

Roßnagel, A. 2007. *Datenschutz in einem informatisierten Alltag*: *Gutachten im Auftrag der Friedrich-Ebert-Stiftung*, Berlin: Friedich-Ebert-Stiftung.

S. Oliveira, M. I., Barros Lima, Glória de Fátima, and Farias Lóscio, B. 2019. "Investigations into Data Ecosystems: a systematic mapping study," *Knowledge and Information Systems* (61:2), pp. 589-630 (doi: 10.1007/s10115-018-1323-6).

Shapiro, C., and Varian, H. R. 1998. *Information rules: A strategic guide to the network economy*, Boston, Mass.: Harvard Business School Press.

Simon, H. A. 1955. "A Behavioral Model of Rational Choice," *The Quarterly Journal of Economics* (69:1), p. 99 (doi: 10.2307/1884852).

Simon, H. A. 1956. "Rational choice and the structure of the environment," *Psychological review* (63:2), pp. 129-138 (doi: 10.1037/h0042769).

Simon, H. A. 1997. *Models of bounded rationality: Empirically grounded economic reason*, Cambridge: MIT Press.

Sinnreich, A., and Gilbert 2019. "The Carrier Wave Principle," *AoIR Selected Papers of Internet Research* (doi: 10.5210/spir.v2019i0.11035).

Snowden, E. 2019. *Permanent record*, London: Macmillan.

Solove, D. J. 2020. "The Myth of the Privacy Paradox," *GW Law Faculty Publications & Other Works* (1482) (doi: 10.2139/ssrn.3536265).

Spiekermann, S., Acquisti, A., Böhme, R., and Hui, K.-L. 2015. "The challenges of personal data markets and privacy," *Electronic Markets* (25:2), pp. 161-167 (doi: 10.1007/s12525-015-0191-0).

Spiekermann, S., and Korunovska, J. 2017. "Towards a value theory for personal data," *Journal of Information Technology* (32:1), pp. 62-84 (doi: 10.1057/jit.2016.4).

Sunyaev, A., Dehling, T., Taylor, P. L., and Mandl, K. D. 2015. "Availability and quality of mobile health app privacy policies," *Journal of the American Medical Informatics Association* (22:e1), e28-e33 (doi: 10.1136/amiajnl-2013-002605).

Swire, P. P., and Lagos, Y. 2013. "Why the Right to Data Portability Likely Reduces Consumer Welfare: Antitrust and Privacy Critique," *SSRN Electronic Journal* (doi: 10.2139/ssrn.2159157).

Thiebes, S., Dehling, T., and Sunyaev, A. 2016. "One Size Does Not Fit All: Information Security and Information Privacy for Genomic Cloud Services," *ECIS 2016 Proceedings*.

Tiwana, A. 2014. *Platform ecosystems*: *Aligning architecture, governance, and strategy*, Amsterdam, Waltham MA: MK.

Turow, J., Hennessy, M., and Draper, N. 2018. "Persistent Misperceptions: Americans' Misplaced Confidence in Privacy Policies 2003–2015," *Journal of Broadcasting & Electronic Media* (62:3), pp. 461-478 (doi: 10.1080/08838151.2018.1451867).

Tversky, A., and Kahneman, D. 1974. "Judgment under uncertainty: Heuristics and biases," *Science* (185:4157), pp. 1124-1131 (doi: 10.1126/science.185.4157.1124).

Vogt, A. 2019. "Automatisch meins? – Die Rechte an maschinengenerierten Daten," *Bonner Rechtsjournal* (12:2), pp. 77-80.

von Oelffen, S. 2020. "Eigentum an Daten," in *Künstliche Intelligenz*: *Rechtsgrundlagen und Strategien in der Praxis*, J. G. Ballestrem, U. Bär, T. Gausling, S. Hack and S. von Oelffen (eds.), Wiesbaden: Springer Gabler, pp. 77-81.

Waldman, A. E. 2020. "Cognitive biases, dark patterns, and the 'privacy paradox'," *Current opinion in psychology* (31), pp. 105-109 (doi: 10.1016/j.copsyc.2019.08.025}).

Wiebe, A. 2016. "Protection of industrial data - a new property right for the digital economy?" *GRUR Int.* (65:10), pp. 877-884.

World Economic Forum 2011. "Personal Data: The Emergence of a New Asset Class," Geneva, CH.

Zhou, L., Pan, S., Wang, J., and Vasilakos, A. 2017. "Machine Learning on Big Data: Opportunities and Challenges," *Neurocomputing* (237), pp. 350-361 (doi: 10.1016/j.neucom.2017.01.026).

Zrenner, J., Moeller, F. O., Jung, C., Eitel, A., and Otto, B. 2019. "Usage control architecture options for data sovereignty in business ecosystems," *Journal of Enterprise Information Management* (32:3), pp. 477-495 (doi: 10.1108/JEIM-03-2018-0058).

Zuboff, S. 2019. *The age of surveillance capitalism*: *The fight for a human future at the new frontier of power*, New York: PublicAffairs.

Zuiderwijk, A., Janssen, M., van de Kaa, G., and Poulis, K. 2016. "The wicked problem of commercial value creation in open data ecosystems: Policy guidelines for governments," *Information Polity* (21:3), pp. 223-236 (doi: 10.3233/IP-160391).