Sovereignty and Data Sharing

SOVEREIGNTY AND DATA SHARING

Patrik Hummel[1], Matthias Braun[1], Steffen Augsberg[2], Peter Dabrock[1]
[1]Friedrich-Alexander-Universität Erlangen-Nürnberg, Department of Theology, Germany
[2]Justus-Liebig-Universität Gießen, Department of Law, Germany

Abstract *– In this paper, we characterize the notion of data sovereignty as a normative reference point for information and communication technology (ICT) governance. We explain why in our view, establishing data sovereignty means more than securing privacy, but also requires the availability of controllable means for sharing information with others. We argue that in the context of big data applications, dynamic consent mechanisms play a key role in steering information flows in accordance with the proposed normative reference point. We close by suggesting legal and governance aspects of implementing data sovereignty: explorations of data ownership notions, aiming at data literacy in education, encouraging transparency about data processing activities, and introducing representative data agents that channel data flows in accordance with individual preferences.*

Keywords – Data agents, data ownership, data sharing, privacy, sovereignty

1. INTRODUCTION

At the World Economic Forum 2018, Yuval Noah Harari began his speech by highlighting that data has become the most important asset in the world [1]. Data will take on the role that land played in ancient times, and machinery has in the last few centuries. It will be the basis for the main products of the 21st century economy: not textiles, vehicles and weapon, but bodies, brains, and minds. Those who own and control data, Harari claims, will shape the future not just of humanity, but the future of life itself.

If we anticipate data to attain the status Harari envisions, questions arise about how to make use of this resource, how to allocate it, manage access and usage rights, and maximize its potentials, e.g., for research, health, sustainable development, and economic growth. In order to pursue these ends responsibly, data should be leveraged towards a better and more just future in which it benefits everyone. We are witnessing the age of digitization, big data, automation, and algorithmic data processing. Radically new ways to gather, access, and interpret data are emerging. Information and communication technologies (ICTs) both generate data and are the locus of data processing. This double aspect of their data intensity makes ICTs a crucial target area for responsible engineering and governance frameworks.

In this paper, we characterize the notion of data sovereignty as a normative reference point for ICT governance (2.). We explain why in our view, establishing data sovereignty means more than securing privacy; it also requires the availability of controllable means for sharing information with others (3.), ideally on the basis of dynamic consent mechanisms (4.). We close by suggesting legal (5.) and governance (6.) aspects of implementing data sovereignty.

2. DATA SOVEREIGNTY AS A NORMATIVE REFERENCE POINT

As the deployment of big data applications and artificial intelligence intensifies across a variety of sectors, one up-and-coming concept in discourses on responsible governance is the notion of data sovereignty. Although not used uniformly throughout the literature, the concept relates to issues of control about who can access and process data [2–5]. Historically, sovereignty denotes claims to absolute power relative to a domain, e.g., the power of a sovereign nation state in its territory. Calls for data sovereignty transfer this picture to the realm of data and ICT: sovereign data subjects are those who are in a position to articulate and enforce

claims to power about their data. Governance shall strive to make individuals data sovereigns.

One important clarification is immediately in order. Taking sovereignty as a normative reference point is not the same as approving and demanding respect of just *any* claim to power. Compatible with and arguably inherent to the concept of sovereignty is a relational aspect: whether a claim to sovereign power is legitimate depends on its content and the relationship between the putative sovereign and her claim's addressees. If arbitrariness or unreasonable self-interest drive the claim, sovereignty turns into despotism. Negotiating sovereignty and its scope is a discursive process to be carried out in dialogue with others and society.

With this in mind, we can distinguish two levels on which data sovereignty can be impaired. Firstly, the sovereignty of *nation states* appears compromised by challenges and perplexities of *aligning* [6] the online world (or parts thereof) with national legislation. For example, commentators worry that governments which use cloud computing could store data outside their jurisdiction and run the risk of compromising national sovereignty by conceding control over information [7]. This is why some authors identify data sovereignty with the ability to geolocate data, to place it within the borders of a particular nation state [8], and to resolve uncertainty about which laws apply [9].

Secondly*, individuals* cease to be data sovereigns if they are unable to articulate or enforce claims to power and/or if they are unaware of the flow of their personal information, the nature of the data that is being generated about their lives, who can access it, the ways in which it is processed, and the mechanisms in which such processing feeds back into their decision making. In the worst case, potentially autonomous and reflective subjects are degraded to mere objects of data flows.

In this context, caution is needed against a looming *granularization* of human dignity [10]. Big data tools, algorithms, and neural networks continuously recognize patterns and reduce our lives to conglomerates of data points, which themselves can be rearranged and set into relation to other fine-grained data sets: linkages unite social media data, shopping behavior, traffic data, health records, forensic records, political attitudes, financial transactions, and more. These developments threaten to compromise human dignity in at least two ways: first, the linkages make data processing more invasive than ever and result in an unprecedented degree of transparency of the individual. Second, these tools are not limited to capturing, describing, and analyzing us and our activities. Our lives become *shaped* by them. There is a spectrum ranging from harmless nudging to potentially more egregious interferences with decision making and even preference formation. The worry is that self-determination and autonomy come under fire, and that the ideal of data sovereignty becomes unattainable.

3. BEYOND PRIVACY?

A variety of definitions of privacy exist. It is one of the most prominent values invoked against threats of overly invasive and manipulative interventions. For example, Luciano Floridi describes privacy as a function of *informational friction*, i.e. "the forces that oppose the flow of information" [11]. The more this flow is constrained, the less accessible information becomes to others.

Privacy could be understood as merely a protective and constraining concept. While acknowledging the importance of privacy in this sense, the normative reference point of data sovereignty goes beyond it. On the one hand, data restrictiveness can express self-determination, focused on individual rights exercised in ways that *exclude* others from one's informational sphere. On the other hand, data *sharing* can be the expression of solidarity, orientation towards claims of others, and commitment to the common good. Data sovereignty reflects that individual decision making mediates between restrictiveness and sharing without categorically privileging either. The notion thus demands that privacy protections are complemented by controllable methods for weaving informational ties to others [12].

This being said, there is overlap between privacy and data sovereignty, e.g., if privacy involves the "claim of individuals, groups, or institutions, to determine for themselves when, how, and to what extent information about them is communicated to others" [13], or more generally if it means "control over personal information" [14]. These notions take the individual as the basic unit of analysis. Something similar goes for the Fair Information Practice Principles [15] which specify individual rights related to accessing, amending, and controlling data, and have shaped legislation in the

United States and beyond. Data sovereignty, on the other hand, takes as a starting point the social and collective setting in which individual claims are being articulated, recognized, and respected. Privacy understood as contextual integrity [16], where the appropriateness of information flows turns on context-relative expectations and norms governing access, is mindful of the social embeddedness of privacy claims. But unlike data sovereignty, it appears to leave positive entitlements to share information unarticulated.

Two examples illustrate that such entitlements are vital. First, our lifeworlds are increasingly digitized and mediated by data. Floridi and others [17] use the term *onlife* to capture the intertwining, fusion and indivisibility between our analogue, offline lives and our ICT-driven activities and self-understandings. While privacy protects individuals against misuse of their data, Floridi argues that its primary importance flows from our status as "informational organisms (*infogs*), mutually connected and embedded in an informational environment (the infosphere)" [11]. Because of the significance of information for the self-constitution of *infogs*, privacy breaches infringe upon their identity. This is what Floridi suggests constitutes the distinctive wrongness of such breaches.

Still, violating privacy is just one way of wronging *infogs*. Compatible with and arguably inherent to the proposed picture is that the integrity of *infogs* requires not only protections but also entitlements. Privacy protects a deeply personal sphere, but the personality and identity residing in this sphere is itself constituted by informational ties and relations to others. It is the sharing, not the retention of information that constitutes identities in the first place. *Infogs* conceive of themselves and re-identify as well as recognize each other on the basis of information flows which catalyze social bonds that are constitutive of a fulfilled life. Indeed, intimacy and closeness are paradigmatically located in areas where informational friction is *suspended* in the right ways. As Floridi illustrates, upon returning to Ithaca, Odysseus is recognized by his wife Penelope on the basis of his knowledge of information that only the two of them have in common.

Second, sharing data is vital in many contexts where we hope to enjoy the benefits of state-of-the-art technology. For example, personalized medicine requires the availability of large amounts of data in order to stratify and tailor services towards the individual. In these contexts, and especially in cases of rare disease, a patient's decision to share her data directly affects the clinical prospects of others. With the emergence of artificial intelligence in the clinic, patient data is being used to learn neural networks designed to improve quality, speed, and resource efficiency of clinical decision making and treatments, e.g., on personalized cancer therapy [18]. With the rollout of electronic health records, sharing one's personal health data has become easier than ever.

In this context, we can also mention the increasingly popular concept of a l*earning healthcare system* [19] which seeks to embed knowledge generation into clinical care, including the systematic consideration of routine clinical data in evidence bases and research processes. Some authors see an "obligation of patients to contribute to the common purpose of improving the quality and value of clinical care and the health care system" [20].

If one prefers to be more careful [21] with regards to a duty to participate in endeavors of this kind, one fruitful avenue is to examine the range of attitudes and dispositions which subjects bring to the table all along. Gift theorists maintain that certain acts of giving are fully understood only if we recognize their *aneconomic* aspects: These acts involve a sense of endowment, are being carried out without the intention to prompt a return, transcend the individual's self-interest, and convey a symbolic, non-commodifiable aspect that encodes the donor's dedication and investment of a part of *herself* into what she is giving [22–24]. In these ways, gifts present elements of recognition that cannot be offset against other things and introduce these elements into interactions that otherwise would be guided primarily by a logic of economic exchange.

Health-related acts of giving impact the recipient in an immediate and bodily way, and the donation of personal health data is no exception. For example, genomic data is highly intimate and essentially personalized, yet some individuals obtain their genomic data from direct-to-consumer genetic testing and proceed to share it with researchers and even the public domain. Empirical evidence on the motivation of these individuals suggests that they are aware of looming privacy risks, but besides curiosity and the desire to learn more about their genomes, the sharing is driven by the intention to contribute to medical research and to improve

genetic testing and prediction [25].

We propose that once donations are examined through the lens of gift theories, it becomes apparent that they can generate social bonds, convey recognition and open up new options in social space, for example by interrupting patterns of economic exchange and enabling activities and interactions that would have otherwise remained unlikely or impossible [12]. If these potentials are realized, donations can advance individual sovereignty by reinforcing the social structures in which the individual leads her life.

Our claim is not that sharing data is the only way to advance data sovereignty. However, through their acts of giving, donors can enact beneficence, solidarity [26], and shape scientific processes. Proponents of *citizen science* even speak of a human right to participate in scientific knowledge generation [27]. If data subjects are to be sovereigns, the positive dimension of sovereignty thus calls for ways to *facilitate* the sharing of data.

This does not mean that privacy claims shall be deflated, and that people *must* share. It is perfectly compatible with the proposed normative reference point that individuals exercise data sovereignty in restrictive ways and *refrain* from sharing. It does mean, however, that ICT regulators and system designers should also think carefully about room for maneuver for those who, under suitable circumstances, prefer to share rather than to withhold data. The *controllability* of data flows, including the ability to protect, share and retract information, should be at the center of responsible governance.

4. INFORMATION PROCESSING IN BIG DATA REGIMES

In the context of big data and automated information processing, the significance of individual data points cannot be fully understood in isolation. How informative they are depends on whether and how they are conjoined with other data points and sets.

Data undergoes *de- and re-contextualized* faster, more easily, and more frequently than ever. The character of data points is in constant flux. One of the clues of big data tools is that they seek to identify correlations that are *ex ante* unforeseen [28]. This means that individuals are bound to be unaware of the future use of data which they might otherwise willingly share in the present.

The power of data processing technologies as well as tendencies of market concentration in the data processing domain pave the way for *cumulative effects* [29] between data from different domains of our lifeworlds. As mentioned, nearly all parts of our lives and activities are datafied. Linkages amongst datasets make boundaries blur and the sphere of personal secrecy shrink.

Consent to data processing is supposed to allow individuals to exercise autonomy and self-determination as well as to protect them from harms. If future use cannot be fully transparent to the data subject in the present, and if one piece of information, once conjoined with others, can give away much more than the data subject foresees, what should we make of the individual's consent to the processing of her data? For example, to what extent does consent to the terms and conditions of a social media provider justify the inclusion of customer data into epidemiological analyses [30]?

To some extent, such challenges are reminiscent of discourses on the ethics of biobanking where it is antecedently open which research will be carried out with biological specimens. One proposal is to seek broad consent from specimen donors for a variety of research endeavors that remain unspecified at the time of donating the sample. While some defend such models, others criticize them for sacrificing the requirement of informedness that is vital towards exercising self-determination [31]. Another option is to seek *tiered* consent that authorizes the use of a sample towards a range of broadly defined research areas. Unfortunately, in our context, the very notion of a *tier* is deflated in view of the cumulative effects just characterized. If data *tiers* fuse and intertwine sooner or later, it might be mere window dressing to suggest that data subjects can realistically consent to only some particular *tiers* of data processing.

Difficulties like these motivate consent forms that are *dynamic* [32]. Individuals' preferences can be expected to change over time, for example if technological advances open up new possibilities for drawing inferences from a given dataset. This calls for *refined* and *real-time* control mechanisms that allow individuals to provide and withdraw data in accordance with their evolving preferences. One

initial step in this direction is the notion of data portability, i.e. the right to receive personal data and to transfer it from one provider to another, which has found its way into the EU General Data Protection Regulation (GDPR). As Vayena and Blasimme paraphrase, mechanisms like this seek to turn data subjects into data *distributors* [33].

These are positive developments in view of the foregoing insights on the embeddedness of *inforgs*, whose privacy is essential to their integrity, but who also demand ways to share information with others and sometimes even donate data for the greater good. What could regulators and designers of ICT systems do to promote such activities and to put users in a position to exercise, maintain, and modify dynamic consent? We now formulate suggestions for two domains.

5. LEGAL RAMIFICATIONS

Given that technology keeps evolving at an ever-increasing pace, regulators are faced with an uphill struggle. This is demonstrated by the intensity of the current debates about the GDPR and its ability to ensure the right to privacy under big data conditions. With regard to data sharing, another problematic aspect has to be addressed: contrary to popular belief and some misleading semantics, under the current regulatory regime there is no *ownership* of data. The legal concepts of ownership and property are restricted to objects and real estate, and the specific provisions of intellectual property (IP) law do not cover mere data [34]. This does not mean, however, that there is no need for clear rules regarding who has control over data access and data use and who can profit from them. Quite the contrary is true. If we keep in mind that under the law as it stands, the consent model serves as a substitute for more advanced usage rights, it becomes obvious that the development of complex and dynamic consent mechanisms already goes a long way to reduce friction. And yet even more innovative solutions are both imaginable and desirable. In order to safeguard the data subjects' sovereignty, supplementary legal mechanisms are needed to ensure that personal rights as well as rights to freedom can be enacted, remain respected, and become legally enforceable if necessary. One of the strategies discussed by legal experts is the introduction of genuine data ownership in the property sense [35]. Data is behavior-generated and thus encompasses a cultural ontological status beyond its status as mere binary code, which can be taken to motivate *sui generis* laws that codify the agent's ownership of the data she generates [36]. The problem with this approach is, however, that due to the factual differences between data and objects, this would currently be a property in title only. Additionally, since the EU so far does not have a comprehensive competence for this area, such legislation would have to be limited to the national sphere. Another, maybe more promising strategy involves the proxy/agency model already familiar from dynamic consent in which proxies or representatives make decisions on behalf of the data subject (cascading consent) [4,5]. The idea here is to employ surrogate notions for ownership in the property sense. This could help to enable data subjects to (re)gain and sustain control over their data even without the pains of strenuous and time-consuming individual supervisory efforts.

6. PATHWAYS FOR GOVERNANCE

Indeed, attempting to make ICT users data sovereigns can appear to overburden the individual. Ordinary users cannot be expected to have a clear picture about the complexities of ICT, all the pathways that their information takes, and the sophisticated algorithmic analyses and adjustments that are based on the tracks they leave in the infosphere. We simply might be asking for too much if we demand each ICT user to be data sovereign, threaten to overestimate the amount of responsibility that should be ascribed to individuals for their own data integrity, and open the door to holding them partially responsible for privacy breaches and unconstrained information flows.

The worry can be addressed by highlighting that while data sovereignty is a feature that is eventually realized in the individual ICT user, the factors that enable data sovereignty extend beyond the particular data sovereign. They are tied to a multitude of agents and levels. Governance mechanisms that strive to realize the normative ideal of data sovereignty thus need to be multidimensional [4,5].

Individuals themselves are entitled to be provided with education that enhances their literacy with regard to data infrastructures [37]. They cannot be sovereigns if they proceed under ignorance of central features and abilities of the technology they are using. Critical reasoning and power of judgment are key to evaluate the consequences, risks, and

benefits of data-restrictive choices and data sharing respectively.

Still, individual caution and data-restrictive choices only lead so far. It is up to regulators and data processing organizations to ensure that easy-to-understand information on data-intensive ICT is available and disseminated. In particular, careful reflection is needed on how the ideal of transparency could be attained. Transparency can imply disclosure. However, requirements to disclose technological designs, code, and data processing algorithms raise several difficulties. First, even if disclosed, such information remains unintelligible to the lay user, and thus does not advance her informedness. To some extent, terms and conditions suffer from this problem as well: everybody accepts them, almost nobody reads them, and only some of those who read them understand them. Disclosure of code, just as terms and conditions, would have to be complemented by societal discourses with a variety of stakeholders and experts. Only then can the disclosure of complex technical contents end up guiding the non-expert user. Second, even partial mandates to disclose codes and algorithms can affect business interests and incentives for innovation on the side of the ICT providers, e.g., if this *de facto* compromises protections of IP. A more promising avenue is to mandate disclosure of the purposes and aims of a given algorithmic tool. This would make it possible for outsiders to get an idea of the intended functioning of the tool, and to assess whether it works as advertised, e.g., reaches the intended goal with the proclaimed precision and without undue discrimination against certain populations [4,5].

Moreover, disclosure by itself is unhelpful if individuals lack room for maneuver. Amongst the features of the platform economy is that its players benefit from economies of scale and network effects which sooner or later lead to market concentrations [10]. This effectively constrains the choices of individuals for moving from one platform to another. As *infORGs*, it is out of the question for individuals to refrain from using ICT services. One condition of data sovereignty is thus that policy and lawmakers find ways to uphold competition and ensure that the market offers a plurality of data-intensive services from providers with different privacy and control mixes. This also involves discourses on the pricing of data [38] in order to compensate individuals for value generated through the processing of their information.

In the end, data gathering and processing organizations are the entities who develop and implement innovations, and who determine the extent to which users can be data sovereigns. Service providers can support this process through technological infrastructures that allow the individual to control the flow of her data. In the ideal case, data processing rests on the informed consent of the individual whose data is being processed, while she retains options to withdraw consent and mandate deletion of her data from the service provider. Controllability would go a long way towards harmonizing the benefits of big-data-driven de- and re-contextualization with the privacy and expectations of individual data subjects.

Governments can take on a key role in this process, by encouraging the self-regulation of organizations. For example, independent, industry-wide data audit and certification centers can make responsible data management visible. Where self-regulation is lacking, the state can take over through regulation, monitoring, and sanctions. The GDPR is the most recent example of the range of instruments that can be employed internationally while leaving individual nation states discretion to spell out the precise nature of these tools in their jurisdiction.

The rollout and alignment of technological standards for data interoperability and programmatic interfaces is an important area where industry and policymakers can work together to harness data. Uniform standards and formats for exchanging and connecting data from a variety of sources and between different systems make data comparable and translatable. It also facilitates quality control and documentation.

Data interoperability and tools to link, organize, filter, and curate data efficiently [39] can yield significant benefits towards the normative ideal of data sovereignty. First, interoperability is key to data sharing. Lack of interoperability does not necessarily threaten privacy, but it does compromise potentials for exchanging data, a challenge for example in endeavors to utilize routine clinical data for medical research [40]. Second, while standardization does not by itself advance data sovereignty, it sets the stage for introducing technological solutions that help individuals to control the flow of their data.

Architectures such as personal data stores [41] enable users to monitor and administer personal information and metadata, and thus offer ways to implement dynamic consent mechanisms. In addition, trustee and delegation systems can act as data agents or brokers, i.e. mediate between data subjects and processors. Such agents would effectively take on a representative or proxy role and thus extend the reach of individual consent as described above. The behavior of the data agent is based on predefined rules on how to handle and administer data, including storage duration, deletion, exchanges, and anonymization. These rules are set by the individual herself or by other representative bodies such as consumer protection agencies. The data agent also supervises and records exchanges of data, and facilitates rollbacks if necessary [42]. The system requires auditing procedures to monitor and ensure its proper functioning and accordance with the interests of the data subject it shall represent. Once a user-friendly interface is in place, data agents promise to reduce complexity and effort by serving as reliable and convenient instruments for individuals to handle their data. Such systems avoid unreasonable technical burdens and cumbersome decision making on each and every instance of a potential act of data sharing.

Blockchain technology offers further innovative avenues for controlling and channeling data flows. Administration is decentralized, peer-to-peer, and hard to manipulate due to cryptographic backward links between blocks. Data added to the blockchain can encode metadata such as origin, quality, and the extent of consent to processing [4,5], resulting in immutable audit logs reflecting an individual's preferences. The technology could thus in principle be used towards enhancing controllability and data sovereignty. For example, there are proposals to equip patients with cryptographic keys to their health records in the blockchain, and thereby empower them to full control (e.g., through a smartphone app) over who can access what kind of data over which period of time [43].

Despite the justified enthusiasm for blockchains, they also poses challenges. As Primavera De Filippi [44] explains, blockchain technology has its roots in emancipatory and even somewhat subversive movements that intended to use cryptographic technologies for the sake of individual freedom and data protection, particularly against governments. These liberating intentions contrast with market concentrations and emerging power asymmetries that many blockchain technologies witnessed in the recent past. For example, a very small number of mining pools dominate the majority of the bitcoin network. More generally, even technologies intended as decentralized and disruptive can be dominated by a small number of players.

The question of which technologies and designs increase or constrain data sovereignty deserves ongoing critical and multidisciplinary reflection. It might turn out that existing approaches, if applied wisely, already go a long way towards capturing and enforcing dynamic consent. Further research is needed to compare longstanding and novel tools, the benefits they offer, and the trade-offs they involve relative to different use cases.

In light of the foregoing, we suggest that a paradigm shift is necessary. Traditional approaches like consent forms and data-sharing agreements tend to be *input-oriented*: they set constraints at the beginning of data gathering and processing. What seems called for in view of big data and its de- and re-contextualization that obscures future use is *output-orientation* [10]: making sure that the freedom, claims, preferences, and values of data sovereigns are respected when the downstream effects of data-intensive ICT affect their lives.

7. OUTLOOK

We have proposed the notion of data sovereignty as a normative guiding principle for ICT development and frameworks. Responsible and ethically sound informational governance guards individual privacy, but also goes beyond establishing informational friction. The concept of data sovereignty encompasses entitlements of the individual to connect and share information with others. It thus demands not merely constrainable but *controllable* data flows. Once implemented, data sovereignty honors individual autonomous decision making while being mindful of legitimate business interests and incentives for responsible innovation. We highlighted a range of measures in law and governance more broadly conceived that can advance this process: explorations of data ownership notions, aiming at data literacy in education, encouraging transparency about data processing activities, and introducing dynamic consent models, as well as representative and proxy systems that channel data flows in accordance with individual preferences.

Much of Harari's vision mentioned at the outset is dystopian. He argues that the merging of ICT and biotechnology has already given us the ability to "hack" lifeforms, and that one day ubiquitous and invasive data gathering will make human beings easy targets for "hacks" that end up constraining their freedom as well as establishing and sustaining new power structures. From the perspective of the normative reference point of data sovereignty, is it necessary to draw such dystopian conclusions? Given the argument within this paper, there is no question that Harari's poignantly articulated diagnoses and challenges will be amongst the central concerns of discourses on the responsible development of technological innovations for many more years to come. But regarding the prognostic aspect of Harari's vision, the normative reference point of data sovereignty could be a promising first step towards navigating the possibilities of ICT in a responsible, forward-looking, and hopeful manner.

ACKNOWLEDGEMENT

We are grateful for funding from the German Federal Ministry of Health (ZMV/1 – 2517 FSB 013).

REFERENCES

[1] Harari YN. Will the Future be Human? Davos: World Economic Forum 2018. https://www.youtube.com/watch?time_continue=202&v=hL9uk4hKyg4.

[2] Friedrichsen M, Bisa P-J. Digitale Souveränität: Vertrauen in der Netzwerkgesellschaft. Wiesbaden: Springer VS; 2016.

[3] De Mooy M. Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data: Considerations for Future Policy Regimes in the United States and the European Union. Bertelsmann Stiftung; 2017.

[4] German Ethics Council. Big Data und Gesundheit. Datensouveränität als informationelle Freiheitsgestaltung. Berlin: German Ethics Council; 2017.

[5] German Ethics Council. Big Data and Health. Data Sovereignty as the Shaping of Informational Freedom (Executive Summary & Recommendations). Berlin: German Ethics Council; 2017.

[6] Mueller M. Will the Internet Fragment?: Sovereignty, Globalization and Cyberspace. Cambridge: Polity Press; 2017.

[7] Irion K. Government Cloud Computing and National Data Sovereignty. Policy & Internet 2013;4:40–71.

[8] Peterson ZNJ, Gondree M, Beverly R. A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud. Proceedings of the 3rd USENIX Conference on Hot Topics in Cloud Computing, Berkeley, CA, USA: USENIX Association; 2011.

[9] De Filippi P, McCarthy S. Cloud Computing: Centralization and Data Sovereignty. European Journal of Law and Technology 2012;3.

[10] Dabrock P. Die Würde des Menschen ist granularisierbar. Muss die Grundlage unseres Gemeinwesens neu gedacht werden? Epd-Dokumentation 2018;22/18:8–16.

[11] Floridi L. The Fourth Revolution: How the Infosphere is Reshaping Human Reality. Oxford: Oxford University Press; 2014.

[12] Hummel P, Braun M, Dabrock P. Data Donations As Exercises Of Sovereignty. In: Krutzinna J, Floridi L, editors. The Ethics Of Medical Data Donation, Cham: Springer; forthcoming.

[13] Westin AF. Privacy and Freedom. New York: Atheneum; 1967.

[14] Solove DJ. Understanding Privacy. Cambridge, Massachusetts: Harvard University Press; 2008.

[15] U.S. Department of Health, Education & Welfare. Records, Computers, and the Rights of Citizens. Report of the Secretary's Advisory Committee on Automated Personal Data Systems. 1973.

[16] Nissenbaum H. Privacy in Context: Technology, Policy, and the Integrity of Social Life. Stanford, California: Stanford University Press; 2009.

[17] Floridi L, editor. The Onlife Manifesto: Being Human in a Hyperconnected Era. Springer Open; 2015.

[18] Yang Y, Fasching PA, Tresp V. Predictive Modeling of Therapy Decisions in Metastatic Breast Cancer with Recurrent Neural Network Encoder and Multinomial Hierarchical Regression Decoder. 2017 IEEE International Conference on Healthcare Informatics (ICHI), 2017, p. 46–55.

[19] Institute of Medicine. The Learning Healthcare System: Workshop Summary. Washington, D.C.: The National Academic Press; 2007.

[20] Faden RR, Kass NE, Goodman SN, Pronovost P, Tunis S, Beauchamp TL. An Ethics Framework for a Learning Health Care System: A Departure from Traditional Research Ethics and Clinical Ethics. Hastings Center Report 2013;43:16–27.

[21] Bialobrzeski A, Ried J, Dabrock P. Differentiating and Evaluating Common Good and Public Good: Making Implicit Assumptions Explicit in the Contexts of Consent and Duty to Participate. PHG 2012;15:285–92. doi:10.1159/000336861.

[22] Bedorf T. Gabe, Recht und Ethik in Hénaffs anthropologischer Genealogie der Anerkennung. Westend 2010;7:123–32.

[23] Hénaff M. The Price of Truth: Gift, Money, and Philosophy. Stanford, California: Stanford University Press; 2010.

[24] Hénaff M. Ceremonial Gift-Giving: The Lessons of Anthropology from Mauss and Beyond. In: Satlow ML, editor. The Gift in Antiquity, Chichester: Wiley-Blackwell; 2013, p. 12–24.

[25] Haeusermann T, Greshake B, Blasimme A, Irdam D, Richards M, Vayena E. Open sharing of genomic data: Who does it and why? PLOS ONE 2017;12:e0177158.

[26] Prainsack B, Buyx A. Solidarity In Contemporary Bioethics—Towards A New Approach. Bioethics 2012;26:343–50.

[27] Vayena E, Tasioulas J. "We the Scientists": a Human Right to Citizen Science. Philos Technol 2015;28:479–85. doi:10.1007/s13347-015-0204-0.

[28] Mittelstadt BD, Floridi L. The Ethics of Big Data: Current and Foreseeable Issues in Biomedical Contexts. Sci Eng Ethics 2016;22:303–41.

[29] Braun M, Dabrock P. Ethische Herausforderungen einer sogenannten Big-Data basierten Medizin. Zeitschrift Für Medizinische Ethik 2016;4/2016.

[30] Mittelstadt B, Benzler J, Engelmann L, Prainsack B, Vayena E. Is there a duty to participate in digital epidemiology? Life Sci Soc Policy 2018;14:9.

[31] Cargill SS. Biobanking and the Abandonment of Informed Consent: An Ethical Imperative. Public Health Ethics 2016;9:255–63.

[32] Budin-Ljøsne I, Teare HJA, Kaye J, Beck S, Bentzen HB, Caenazzo L, et al. Dynamic Consent: a potential solution to some of the challenges of modern biomedical research. BMC Med Ethics 2017;18:4.

[33] Vayena E, Blasimme A. Biomedical Big Data: New Models of Control Over Access, Use and Governance. J Bioeth Inq 2017;14:501–13.

[34] Montgomery J. Data Sharing and the Idea of Ownership. The New Bioethics 2017;23:81–6.

[35] Thouvenin F, Weber RH, Früh A. Data ownership: Taking stock and mapping the issues. In: Dehmer M, Emmert-Streib F, editors. Frontiers in Data Science, Boca Raton: CRC Press; 2017, p. 111–45.

[36] Fezer K-H. Repräsentatives Dateneigentum. Ein zivilgesellschaftliches Bürgerrecht. Sankt Augustin & Berlin: Konrad-Adenauer-Stiftung; 2018.

[37] Gray J, Gerlitz C, Bounegru L. Data infrastructure literacy. Big Data & Society 2018;5:2053951718786316.

[38] Li C, Li DY, Miklau G, Suciu D. A theory of pricing private data. ACM Transactions on Database Systems (TODS) 2014;39:34.

[39] Deng D, Fernandez RC, Abedjan Z, Wang S, Stonebraker M, Elmagarmid AK, et al. The Data Civilizer System. CIDR, 2017.

[40] Nature Biotechnology. Incentivizing data donation. Nat Biotechnol 2015;33:885.

[41] Montjoye Y-A de, Shmueli E, Wang SS, Pentland AS. openPDS: Protecting the Privacy of Metadata through SafeAnswers. PLOS ONE 2014;9:e98790.

[42] Otto B, Jürjens J, Schon J, Auer S, Menz N, Wenzel S, et al. Industrial Data Space. Digital Sovereignty Over Data. München: Fraunhofer-Gesellschaft; 2016.

[43] Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. J Med Syst 2016;40:218.

[44] De Filippi P. "In Blockchain We Trust": Vertrauenslose Technologie für eine vertrauenslose Gesellschaft. In: Augstein J, editor. Reclaim Autonomy, Frankfurt: Suhrkamp; n.d., p. 53–81.