A Delimitation of Data Sovereignty from Digital and Technological Sovereignty

Conference Paper · June 2023

CITATIONS
0

READS
86

2 authors:

Malte Hellmeier
Fraunhofer Institute for Software and Systems Engineering ISST
3 PUBLICATIONS **3** CITATIONS
SEE PROFILE

Franziska von Scherenberg
Fraunhofer Institute for Software and Systems Engineering ISST
2 PUBLICATIONS **0** CITATIONS
SEE PROFILE

A DELIMITATION OF DATA SOVEREIGNTY FROM DIGITAL AND TECHNOLOGICAL SOVEREIGNTY

Research Paper

Malte Hellmeier, Fraunhofer ISST, Dortmund, Germany,
malte.hellmeier@isst.fraunhofer.de

Franziska von Scherenberg, Fraunhofer ISST, Dortmund, Germany,
franziska.von.scherenberg@isst.fraunhofer.de

Abstract

Digital technology significantly impacts our everyday social lives and how we conduct business. This development results in abundant new data generated by people and organizations. Subsequently, future technological instruments must ensure data sovereignty that empowers individuals to maintain control over their data. However, data sovereignty is still blurry and conceptually overlaps with similar terminologies, such as digital and technological sovereignty. From an Information Systems (IS) point of view, delimiting data sovereignty from digital and technological sovereignty is crucial, creating a uniform understanding, especially for data ecosystems. Our study contributes to sharpening data sovereignty with a systematic literature review of 81 articles. It concludes that data sovereignty mainly drives IS activities by protecting data assets on individual and organizational levels. In contrast, digital sovereignty is shaped by digital expertise and interoperability, while technological sovereignty is the broadest concept with regulations and relations on an international level.

Keywords: Data Sovereignty, Digital Sovereignty, Technological Sovereignty, Data Ecosystems, Literature Review

1 Introduction

Over the past years, the concept of sovereignty in the digital realm has increasingly gained attention in the international discourse due to data protection and challenges in climate change. Even 28 % of small and medium companies in the UK confirm that data sovereignty will drive their future decisions over data handling and storage (4D Data Centres, 2018). In Information Systems (IS) research, it is often used in the context of data ecosystems to build software systems and architectures that guarantee control over data. Due to increasing efforts toward digitalization that shape our everyday lives, different actors, amongst them individuals and organizations, recognize the value of data and want to keep control over it to prevent unintended usage on distribution. The importance of using data and technologies in a sovereign way to guarantee a shift into a sustainable society has been recognized (Caravella, Costantini, and Crespi, 2021) and underlined: "With extensive global digitalisation in all areas of society, our data sovereignty becomes a core aspect to ensure economic growth and social justice in Europe and to manage climate change" (AIT, 2022, p. 1). However, companies must face challenges through collaboration and the sharing of data. These companies understand that data is valuable, and sharing it is necessary not only to stay competitive, optimize internal business processes, and create new business opportunities but also to face challenges that single organizations cannot solve independently (Jarke, Otto, and Ram, 2019). Consequently, these developments show the need for more data sovereignty in research and practice.

Researchers have studied data sharing and sovereignty concepts, including their application in systems and organizations. However, the scientific discourse reflects the inaccurate delimitation of data sovereignty from the commonly used notions of digital and technological sovereignty (Micheli et al., 2020). Despite differences in the meaning of data, digital and technological sovereignty exist; past research often uses the concepts as if they were interchangeable or in a wrong way, like introducing data sovereignty with the concepts belonging to digital sovereignty (Lian, 2021). Due to several simultaneous research activities in the last years, IS literature misses an analysis of the near past on how the terms relate and influence each other. Researchers have already pointed to the necessity of an analytic differentiation, identifying and motivating the problem in the context of sovereignty (Couture and Toupin, 2019) to ensure uniform research usage and establish their accurate application in practice.
This study aims to guide future studies in delimitating these terminologies. It reviews the recently strongly rising research field of the quantitatively three most used sovereignty terms in IS research. Therefore, it aims to answer the following key Research Question (RQ) with the help of a literature review:
How can data sovereignty in Information Systems be delimited from digital and technological sovereignty?
Our analysis structures as follows, including concrete contributions to answer the RQ:

(i) Showing the developments of sovereignty in the analog and digital realm and identifying the research gap by reviewing related work (sections two and three).

(ii) Explaining the applied, systematic literature review method with its conditions like search strategy and the conducted procedure to create a final article collection (section four and appendix).

(iii) Visualizing indicators of the relevant literature distribution, showing detailed information of data, digital and technological sovereignty, including their similarities and differences (section five).

(iv) Guiding future research by showing limitations with a discussion on theoretical and practical implications and a conclusion of all findings (sections six and seven).

2 Background

Before diving deeper into the concrete form of different expressions, it is essential to show the foundation of the sovereignty term with its history and meaning in the analog realm.
Bodin (1577) introduced the first definition of sovereignty in the analog sphere that was continuously adapted over time until now (Adonis, 2019). This lead to different characteristics and focus points of sovereignty itself, while it "is generally defined as the supreme authority over a political entity (a polity)" (Couture and Toupin, 2019, p. 2308). In the last decades of the 20th century, the relation of sovereignty with the digital emerged (Grant, 1983). Different notions and conceptualizations have arisen from there, like the dominating concepts of data, digital, and technological sovereignty Not only IS coined these concepts but also related domains from the analog realm formed them over time. That is why the three concepts require a specialized review and a comprehensive analysis to ensure their relevance in a specific domain, in this case: IS research.

3 Related Work

Over time, several publications looked at other sovereignty aspects related to different domains. This chapter presents the most relevant articles on IS-grounded sovereignty terms and their related concepts. It further describes their delimitation to this work.
Starting with the review from Hummel et al. (2021), they analyze the notions of data, digital, and cyber sovereignty, focusing on context, values, and agents of the different terms. The authors selected the articles based on a systematic review and evaluated them, focusing on data sovereignty. In their research, they did not consider further practical implications. Similarly, Pedreira, Barros, and Pinto (2021) conducted a literature review on data, digital, and cyber sovereignty. They concentrate on vulnerabilities and outbreaks in industry scenarios. Whereas Hummel et al. (2021) emphasize the concept of data sovereignty, Pedreira,

Barros, and Pinto (2021) focus on cybersecurity. However, both reviews do not investigate the concept of technological sovereignty, even if the European Commission has positioned it as a political objective (ASD, 2020) and declared it relevant for future technical and non-technical aspects (Maurer et al., 2015). Besides this, Chapdelaine and McLeod Rogers (2021) refer to data and digital sovereignty without researching technological sovereignty. The authors look at technological sovereignty from a legal point of view, especially for media platforms and individuals. Other juridical studies such as Kushwaha, Roguski, and Watson (2020) elaborate on data sovereignty, touching upon the notions of digital and technological sovereignty concerning laws such as the US CLOUD Act and other regulations in different regions such as the UK, Germany, and Poland. Both publications come from the legal field instead of pure IS research. On a national level, Mawere and van Stam (2020) spotlight data sovereignty issues in Africa, especially Zimbabwe, based on the health system to guide local government. Besides information about the concept, the authors also refer to technological sovereignty without referring to digital sovereignty.

In contrast, Asswad and Marx Gómez (2021) discuss the concept of data ownership from an IS point of view. They describe the role of data ownership and point to its advantages and problems, such as the structure of the Internet of Things (IoT) data or missing regulations. Finally, a literature analysis strengthens the results, and the authors use the concept of data ownership relating to data sovereignty in the technical realm.

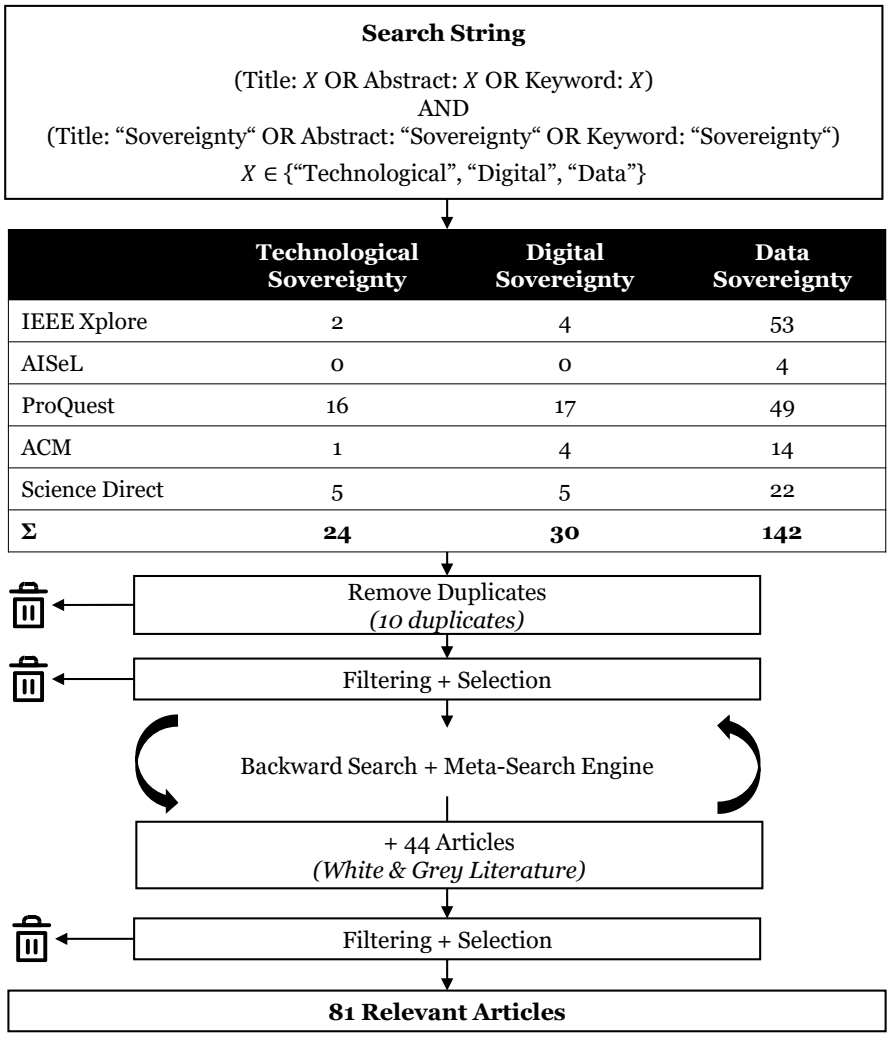
Considering related literature, it becomes clear that from an IS point of view, a detailed analysis of the delimitation of data sovereignty from digital and technological sovereignty does not yet exist. Since cyber sovereignty is also a frequently discussed topic (Hummel et al., 2021; Pedreira, Barros, and Pinto, 2021), it will not be considered further here. Instead, this study analyzes from an IS point of view, and "[t]he fact that the majority of academic literature focuses on the legal implications of sovereignty in cyberspace indicates that the issue of cyber sovereignty is most often framed and understood as a matter of International Law" (Baezner and Robin, 2018, p. 5).

However, literature shows that researchers have made the first steps in describing the terms (Couture and Toupin, 2019). They point to the necessity of the analysis to identify and motivate the problem: "One question that remains open relates to the relationship between different terms" (Couture and Toupin, 2019, p. 2318). In their research, the authors approach a first differentiation of the terms by creating hypotheses on the delimitation of data, digital, and technological sovereignty. They mention that future research must investigate these concepts (Couture and Toupin, 2019). These arguments align with the publication from Mawere and van Stam (2020). Their research cannot constitute a clear differentiation between data and technological sovereignty. In addition, Mawere and van Stam (2020) propose comparing the terms by bringing together different viewpoints to identify their relevance. Therefore, this research extends current work to answer the RQ mentioned above. It closes the gap of the current unspecific delimitation because existing ideas are "[. . .] just hypotheses that would need to be further explored in future works" (Couture and Toupin, 2019, p. 2318). Even though other related concepts are frequently discussed, our quantitative analysis focuses on the IS domains instead of concepts from indigenous people like indigenous data sovereignty (Taylor and Kukutai, 2016) or international law like cyber sovereignty (Baezner and Robin, 2018).

4 Research Design

This study conducts a systematic literature review, analyzing the three most used terms in IS research data sovereignty, digital sovereignty, and technological sovereignty in detail. Since sovereignty aspects are not only relevant to science but also in industry and politics, the present research is based on the recommendations from Webster and Watson (2002) and the guidelines from vom Brocke et al. (2015), extended by a Multivocal Literature Review (MLR). Besides classical reviews on scientific publications (white literature), an MLR increases the scope by including political speeches and technical reports from practitioners (grey literature) to focus on real-world problems due to the combination of academic research and practice (Garousi, Felderer, and Mäntylä, 2019). This study refers to the rationale of Benzies et al.

(2006) to include grey literature, which is, among others, the low quality of evidence. Further, the context for implementing the intervention (Benzies et al., 2006) is vital for sovereignty aspects and strengthens the consideration of publications from practice. Especially in topics around sovereignty whose contexts have policy and industry focus, the inclusion of grey literature provides added value (Benzies et al., 2006). This literature review executes the searches to identify white literature using a keyword-based approach, applied to varying sources to collect journal articles, conference proceedings, and book chapters. Various databases have different key areas and are sometimes limited to specific publishers. This study selected the following five: IEEE Xplore for computer science and technical publications, AISeL and ACM for an IS focus, and ProQuest and Science Direct to include other adjacent domains. In every database, the search strings *technological sovereignty*, *digital sovereignty*, and *data sovereignty* are used, resulting in 15 searches. Every search term is split into its two components (e.g., "data" and "sovereignty") connected with an AND operator to identify literature that divides the words in a text part without using, e.g., "data sovereignty" in one. Here, the title, abstract, and keywords were searched, as Bandara et al. (2015) recommended, without any publication date restriction. The top of Figure 1 shows the resulting numbers based on searches made in April 2022.



	Technological Sovereignty	Digital Sovereignty	Data Sovereignty
IEEE Xplore	2	4	53
AISeL	0	0	4
ProQuest	16	17	49
ACM	1	4	14
Science Direct	5	5	22
Σ	**24**	**30**	**142**

Figure 1. Literature Search Process.

Ten duplicate entries were found in the downstream intermediate step, which led to a reduction from 196 to 186 articles. Here, some entries are listed in two of the five databases, and others are shown two times in

the ProQuest results because this service summarizes 18 databases and can lead to internal duplicates. Due to the precise selection of the databases with mostly disjoint subsets of results, a high number of duplicates is prevented in advance. This first literature set is subject to a full-text scan to check its relevance based on the RQ as the first selection criteria for relevant articles. For this purpose, the texts were searched for the three terms *data sovereignty*, *digital sovereignty*, and *technological sovereignty* and checked if they give a concrete definition, discussion, implementation, or explanation as an inclusion/exclusion criteria. Thus, all articles that do not give new insights about at least one of the three terms, focus on other topics or only mention one term without further details are filtered out. Concerning inter-coder reliability, inconclusive cases are discussed, evaluated, and documented with an exclusion reason in a protocol by the author team to create a final decision and prevent subjectivity.

As described in the recommendations from Webster and Watson (2002), this study applies a backward search of the key literature after the previous filtering step. Here, the authors checked and analyzed all references on the relevant text parts identified in the previous step, whether white or grey literature. At this stage, Kuhrmann, Fernández, and Daneva (2017) suggest extending the primary search with results from a meta-search engine such as Google. This approach supports the inclusion of additional academic publications not listed in the five databases and additional grey literature. It is in line with the MLR guideline seven of Garousi, Felderer, and Mäntylä (2019) that focuses on, e.g., additional web searches. Since many results exist, only 1st tier grey literature with a more known outlet control and expertise is analyzed. It excludes 2nd and 3rd-tier grey literature like Q/A sites, emails, or tweets (Garousi, Felderer, and Mäntylä, 2019). Finally, the authors stopped the process at the theoretical saturation, based on guideline eight of an MLR (Garousi, Felderer, and Mäntylä, 2019). At this stage, this research identifies additional 44 articles for review.

The current white and grey literature collection is subject to the same filtering and selection step described above. The resulting set consists of 81 articles, 52 extracted from the databases and 29 found by the backward search or with the help of the meta-search engine. Besides its content, this study analyzes the collection by tagging every article with metadata such as title, author, publication date, category, source, country of the main authors' institution, and similar facts. The overall process is summarized in Figure 1 to avoid existing concealment problems in IS literature reviews and to ensure replicability (vom Brocke et al., 2009). The final article overview is shown in the Appendix in Table 1 to ensure complete transparency. Upon request, the full list, including all sources and analyzed details like country distribution, is shared to ensure complete repeatability.

5 Results

The following section presents the findings from the systematic literature review with a downstream thematic classification. For this purpose, the authors thoroughly analyzed all relevant articles by extracting the terms' information concerning the RQ.

After a descriptive overview of the literature set, the authors describe data, digital, and technological sovereignty in detail and show their origin and current usages. Based on the RQ, a summary of every term and their relation to data sovereignty can be found in the textbox at the end of every subsection. They are not intended to create a new definition but to conclude the findings from the different descriptions of the articles from the literature review. Subsequently, for the derivation of future action recommendations, all information is analyzed concerning IS research to show the differences between data sovereignty and the other terms depicted in Figure 5.

5.1 Descriptive Findings

Research on sovereignty in the digital realm first occurred in the last decades of the 20th century (Grant, 1983). However, most data, digital, and technological sovereignty publications stem from the last years.

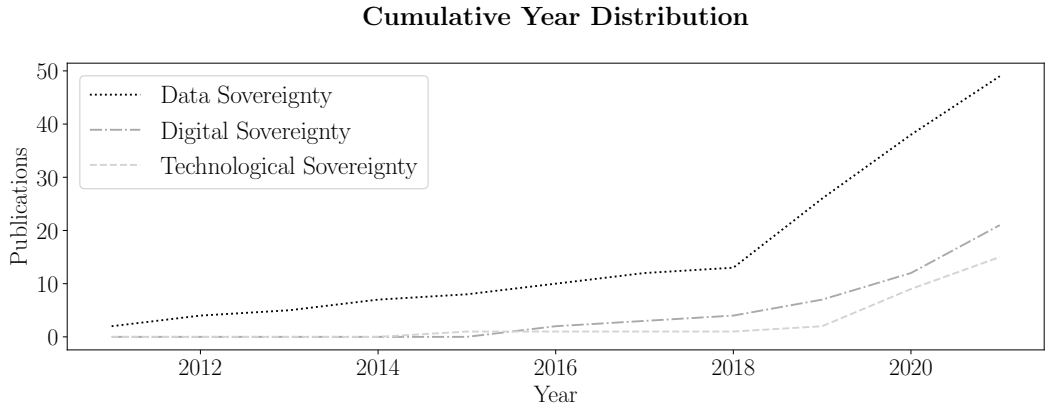


Figure 2. Cumulative Publication Time Distribution of the Past Ten Years on the Relevant Literature Set.

Figure 2 shows the cumulative number of publications for every term in the last ten years based on the relevant literature set from the literature review. Articles are counted in the statistic if they cover one of the three sovereignty aspects. Around 11 % of the scanned literature refers to publications that do not exclusively focus on data, digital, or technological sovereignty but observe more than one term. An example is the research of Pedreira, Barros, and Pinto (2021) that mentions digital and data sovereignty. In this case, the authors counted this paper twice, one time for every category. The graph shows that since 2018, data sovereignty has been the most discussed term, while digital and technological sovereignty are also increasingly gaining attention.

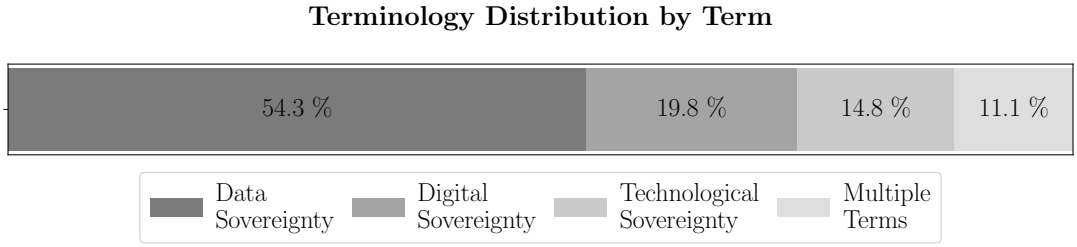


Figure 3. Terminology Distribution on the Relevant Literature Set.

More concretely, 54.3 % of the 81 articles specialize in data sovereignty, while 19.8 % focus on digital sovereignty and 14.8 % cover technological sovereignty, summarized in Figure 3. The rapid simultaneous increase in research further motivates a structured review of past results to guide future research and prevent misunderstandings in the delimitation of the terms.

During the literature search and selection, every article of the final literature set is assigned to a country based on the location of the main authors' institutions to create a location-based distribution of the publications shown in Figure 4. Here, the authors aggregated the countries to their associated continents and rounded the percentage values to whole numbers. While there are no publications from South America and, logically, Antarctica, only one publication from Africa (Mawere and van Stam (2020)) and one from Australia / Oceania (Vaile (2014)) are present. Therefore, the research is mainly conducted in Europe, followed by North American and Asian countries based on quantitative measurement. Most European papers are published by German researchers, followed by publications from France (six papers) and the United Kingdom (six papers). The rest is split up between different European countries like the Netherlands, Belgium, and Italy (three papers each), Finland, and Spain (two papers each), and others with one publication each.

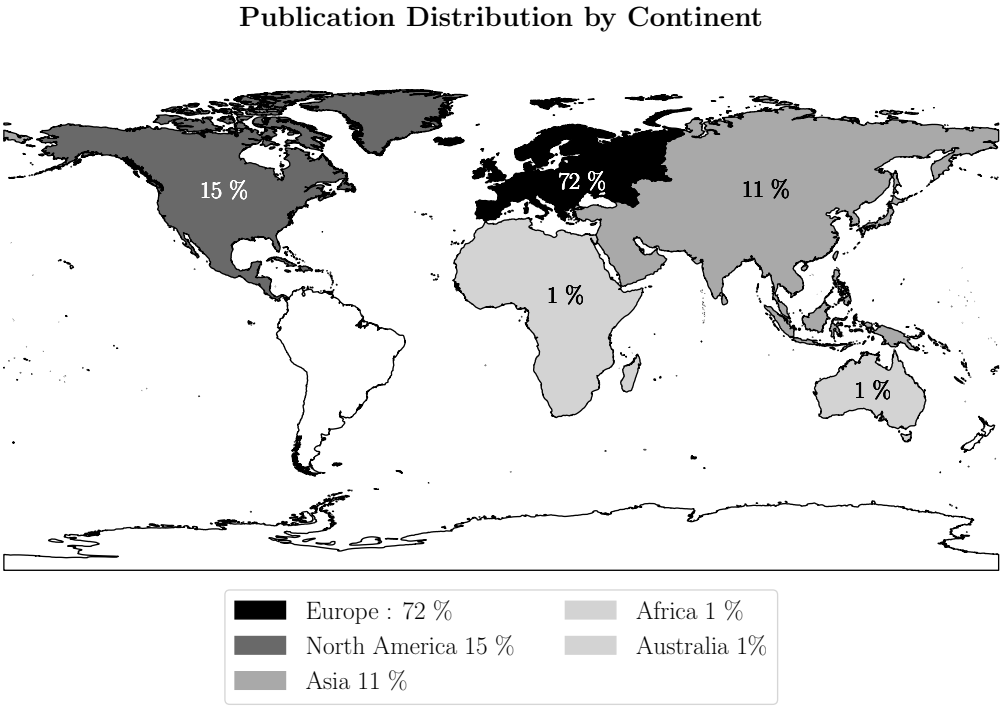


Figure 4. Publication Continent Distribution on the Relevant Literature Set.

5.2 Concepts of Sovereignty

Different conceptualizations of sovereignty terminology in the digital have appeared in recent decades. We focus on the most used notions in IS research data, digital and technological sovereignty. Cyber sovereignty (Couture and Toupin, 2019; Pohle and Thiel, 2020), in contrast to digital sovereignty, comprises the physical dimension of sovereignty in cyberspace (Baezner and Robin, 2018) and constitutes only one aspect of digital sovereignty providing the motivations for the researchers to exclude it from this study' delimitation. The results are formed under the consideration of mixed terms such as digital data sovereignty (Aydin and Bensghir, 2019), personal data sovereignty (Micheli et al., 2020), or urban technological sovereignty (Vadiati, 2022). This study's scope does not include the delimitation of little-used terms such as AI or 5G sovereignty (Floridi, 2020). Besides, the present research does not discuss terms from other domains without a full technical or IS focus, such as indigenous (Taylor and Kukutai, 2016), food, body, or state sovereignty (Couture and Toupin, 2019).

5.2.1 Data Sovereignty

Data sovereignty is the term most used based on the findings of the present literature review (Figure 2). Fifty-one publications of the relevant literature basket form the following results. However, the term lacks a unique definition, and research shows that its usage does not happen consistently (Martens and Zscheischler, 2022; Micheli et al., 2020). It was initially taken up in 2001, with the first ideas mentioned in the US Patriot Act (Hallinan, 2022). When using the term data sovereignty, researchers often refer to what is understood by the concept of (data) self-determination (Banse, 2021; Hummel et al., 2018; Jarke, Otto, and Ram, 2019). The scope of the term is broad and includes different requirements around data, such as confidentiality and data integrity, with the protection against unwanted modifications or data availability (Nugraha, Kautsarina, and Sastrosubroto, 2015). Therefore, it is relevant for individuals and organizations (Jarke, Otto, and Ram, 2019).

For further understanding, the terminology has to be analyzed from an IS and Software Engineering (SE) point of view. In a classical data transfer, a person, organization, or system (referred to as a data provider) shares data with a third party (referred to as a data consumer) and wants to keep control over it (Otto et al., 2019; Zrenner et al., 2019). One example is medical data that belong to a patient (data provider) who can decide and allow access to hospitals or doctors (data consumer) (Plateaux et al., 2013). Since the data have to be secured, data sovereignty means that a data provider can decide and keep control over his or her data. Unfortunately, practice often solves it with written contracts or oral agreements, which regularly fail and can be prevented with technical solutions (Zieglmeier and Pretschner, 2021).
So far, different technical solutions and architectures have arisen that aim to take up data sovereignty ideas. One attempt is the International Data Spaces (IDS) initiative, building up data spaces and data ecosystems based on a reference architecture model to enable sovereign data transfers with the help of different components such as IDS Connectors (Otto et al., 2019). Other ideas are trustworthy architectures (Zieglmeier and Pretschner, 2021), connector-based communication schemes for IoT devices (Qarawlus et al., 2021), blockchain integration (Hong and Kim, 2020), or combinations with other standards such as the Industrie 4.0 Asset Administration Shell (AAS) (Redeker et al., 2020).
Developing systems and architectures or building concepts for technical solutions in IS or SE must meet personal or organizational requirements and comply with the law. In the context of data sovereignty, business and countries formulate requirements in the form of regulations to protect individuals, as seen with the EU General Data Protection Regulation (GDPR), approved in 2016. Such regulations focus on national data sovereignty, a term taken up by Irion (2012), building the transition to digital and technological sovereignty. Therefore, developers, system architects, and researchers must look at data sovereignty and understand other terms and requirements to create compliant data sovereign solutions, even if they are mainly coined by other domains such as economic or political science.

> Concepts of self-determination and the capability of a data provider to keep control over their own data assets form the term **data sovereignty**. Among other things, it is used in the IS and SE domains to create technical solutions to protect individual and company data and highly depends on economic, political, and legal aspects.

5.2.2 Digital Sovereignty

Since the meaning and usage of *digital sovereignty* differ from data sovereignty, the scientific discourse must avoid using both as synonyms. Researchers discuss the concept and its history in detail, shown by the 24 articles of the final literature set. The first ideas go back to the late 1990s. Key events like the Patriot Act in 2001, the Snowden disclosure in 2013, Brexit in 2016, and the COVID pandemic in 2020 formed the term and changed its definitions (Hallinan, 2022). Similar to the other discussed concepts, digital sovereignty has no unique definition because of its changes over time and its dependence on context and stakeholders (Hallinan, 2022).
Due to the formative sociopolitical events during the last years, different nations recognized problems in protecting their citizens in the digital realm that triggered discussions and actions around a nation's digital sovereignty (Pohle and Thiel, 2020). Derived measures include the control and influence of the digital world formed by hardware, software, and infrastructure (Floridi, 2020). However, problems arise because nations can enact local laws and regulations, but cyberspace goes beyond it and covers the whole world. While, for example, governments can regulate the construction of internet cables across borders, the governance of data that flows through it is more complex. Therefore, research coins the attempt to create generalized regulations based on territory and borders regarding data flows as digital sovereignty and accompanying terms such as cyberspace or territorial sovereignty (Cattaruzza et al., 2016; Hallinan, 2022). The study deliberately chooses to analyze digital sovereignty because apart from territorial aspects of cyber sovereignty, it moreover comprises aspects of the digital transformation from a political point of

view (Pohle and Thiel, 2020). Former German Chancellor Angela Merkel further clarified in her speech in 2019: "[...] digital sovereignty does not mean protectionism [...] rather, it describes the ability both of individuals and society to shape the digital transformation in a self-determined way" (Merkel, 2019). Thus, regulations act as an enabler for digital sovereignty because they shape the concept's perception and development.

Besides the political and territorial focus that relates more to control than authority (Cattaruzza et al., 2016), digital sovereignty significantly impacts enterprises and individuals. Businesses and states influence the notion of digital sovereignty in sometimes contrasting ways. On the one hand, companies build, design, and actively participate in the digital realm. In contrast, states use control mechanisms and deploy regulations, sometimes decelerating innovative processes and societal progress (Floridi, 2020). On an individual level, digital sovereignty relates to the concept of interoperability. Another significant element is the freedom to select and use digital assets without being bound to a specific technology (Kagermann, Streibich, and Suder, 2021).

Digital sovereignty focuses on actions, expertise, and control mechanisms in the digital world, while publications often concentrate on territorial borders in the political and economic realm. It helps protect businesses and individuals from selecting and using technology and digital assets in an interoperable way. Regarding data sovereignty, digital regulations, and economic actions are implemented in software systems and directly influence data handling, covered in IS research.

5.2.3 Technological Sovereignty

Regarding the broadest concept, research refers to tech-, technology- or *technological sovereignty* in 17 publications of our gathered literature basket. Its origins go back to the 20th century, with one of the first technological sovereignty definitions described as "the capability and the freedom to select, to generate or acquire and to apply, build upon and exploit commercial technology needed for industrial innovation" (Grant, 1983, p. 240). In these early days, the term referred to the ability of different states to develop, use and produce their technologies and innovations (Couture and Toupin, 2019). The main element that characterizes technological sovereignty is the capability to build techniques and other products, including competencies and licenses. Besides, Grant (1983) describes technological sovereignty as a guarantor of freedom due to reduced dependencies on other states. This assumption is grounded in the fact that licenses and regulations are needed to allow and enable industrial and productive innovations (Grant, 1983).

On closer inspection, these studies assume that states must produce and control all resources and invest in their research as a necessary derivation for building products and infrastructures without external dependencies. However, this feasibility must be questioned because most states can only enable local production and invention with import and export relationships with other countries. For example, rare-earth elements are primarily mined in Asia but are relevant in Europe to build electrical products. European dependencies from the United States in various domains extend a strong international link (Crespi et al., 2021). Therefore, researchers extended the concept of technological sovereignty, which does not mean autarky or complete technological independence (Edler et al., 2021). Cooperations and communication are necessary to build trade relationships and create innovations (March and Schieferdecker, 2021). These aspects can be found in the definition from Edler et al. (2020): "We define technology sovereignty as the ability of a state or a federation of states to provide the technologies it deems critical for welfare, competitiveness, and its ability to act and to be able to develop these or source them from other economic areas without one-sided structural dependency" (Edler et al., 2020, p. 8).

Due to its increasingly linked national and international relations, technological sovereignty became relevant in politics. Since 2019 it has been included in political debates (March and Schieferdecker, 2021) and integrated into political strategies. In her speech in 2020, European Commission's president von der Leyen described it as Europe's capability to make choices based on its values and rules (von der Leyen,

2020). Accordingly, the importance of technological sovereignty can be underlined by its position in the digital strategy of the EU (European Commission, 2020). Concerning the conflict of complete autarky and international trade, technological sovereignty, in the understanding of the European Commission, is a baseline of self-supply extended by solid import and export relationships for resistance against crises such as pandemics, wars or others (ASD, 2020). However, the topic is significant in Europe and other states like Canada, Australia (Couture and Toupin, 2019), Brazil, and China (Maurer et al., 2015). March and Schieferdecker (2021) further summarize these political aspects: "Technological sovereignty is the ability of a polity to self-determinedly shape the development and use of technologies and technology-based innovations which impact its political and economic sovereignty" (March and Schieferdecker, 2021, p. 9). Technological sovereignty includes several trends like data storage location, new undersea cables, localized routing, and others (Maurer et al., 2015).

Technological sovereignty activities focus on a political level with a sometimes national but more international focus. Strategies and regulations influence how sovereign data systems are built. Strong country cooperation relationships support keeping control over resources and influence data sovereignty activities by reducing dependencies.

5.3 Sovereignty in IS Research

As described in the literature overview section, sovereignty has reached momentum in the last few years. The literature review reveals that data sovereignty proves assertiveness in IS research since it describes essential parts of developing technologies.

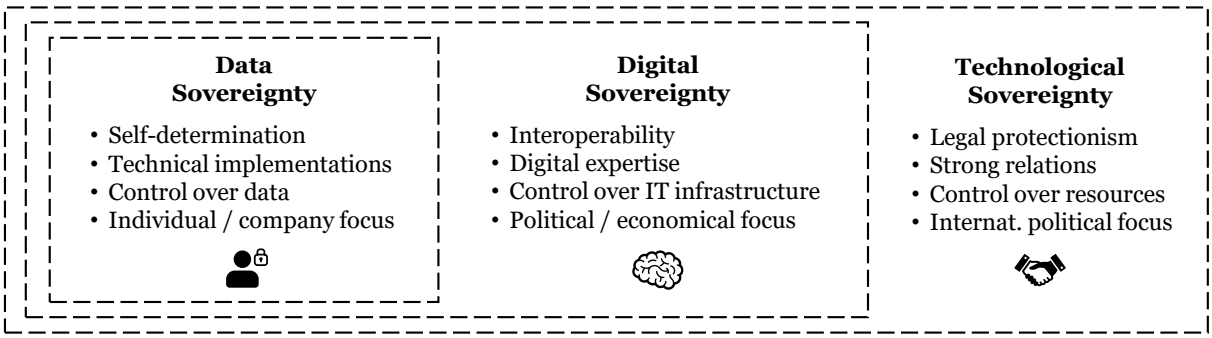


Figure 5. Delimitation of the Analyzed Sovereignty Terms.

A summary of the main characteristics related to IS in the style of Calzada (2021a) is presented in Figure 5. Here, digital sovereignty refers to the digital literacy of a population and the level of development of digitization concepts. Furthermore, it influences IS research through the strong orientation with political and economic focus and their request for more interoperability.

Instead, technological sovereignty, as the broadest concept, is essential in the political discourse, often on an international level, as shown by initiatives from the EU. This concept focuses on the technical usage and sometimes independence of resources from other nations and trade areas with strong relations. It is often associated with freedom and dependencies on political levels.

The review also shows that data sovereignty in IS research, the ability to control individual or organizational data assets, cannot be limited to one research domain. Therefore, observing adjacent fields such as digital or technological sovereignty from an IS point of view is crucial to fully understand how they form and influence the definition of data sovereignty. For example, economic activities and political regulations directly impact system development processes and the definition of data sovereignty. Examples are the recently introduced Data Act on a European level (Perarnaud and Fanni, 2022) or regulations from other

regions like the US CLOUD Act or the Personal Information Protection Law (PIPL) of China. Also, if regulations on an international or national level are discussed for technological or digital sovereignty, they control and shape how data sovereignty can be realized in software and algorithms.

6 Discussion

This IS research-based delimitation of data sovereignty from digital and technological sovereignty, as described in the RQ, serves as a necessity for future research. A mutual understanding of the terms' similarities, differences, and usage is crucial for further developments in the digital economy and SE projects, especially in all data-driven innovations in data spaces and data ecosystems. Since the results from the literature review set a first starting point, implications for theory and practice, as well as limitations and points of contact for future research, have to be discussed.

6.1 Theoretical Implications

Prior research has shown differences between data, digital and cyber sovereignty (Hummel et al., 2021; Pedreira, Barros, and Pinto, 2021). However, the importance of technological sovereignty has increased. It has overtaken cyber sovereignty, as shown by current research activities in the academic domain and the positioning on political levels like the European Commission (ASD, 2020). Especially in IS and SE research, data sovereignty, unlike others, finds a concrete application without a clear delimitation. Since previous work started with assumptions, they motivate future research activities (Couture and Toupin, 2019) concerning a comparison (Mawere and van Stam, 2020).
This study works on the gap by systematically reviewing the past in the academic and practical domains. The results show the theoretical importance, especially since 2018 (Figure 2). Quantitatively, a clear overweighting of data sovereignty with a strong European focus is shown (Figure 4). It strengthens, on the one hand, the need for a clear delimitation, but on the other hand, it poses the question of why some regions are more underrepresented than others. The final thematic classification has implications for future IS activities and other related sovereignty domains, such as political, economic, and legal perspectives.

6.2 Practical Implications

The results show that the different concepts focus on different domains, which leads to direct implications for practice. As stated above, the concepts have strong relationships and influence each other. A geopolitical decision for technological sovereignty acts on digital sovereignty and influences concrete software products and their development process in private and industrial contexts. Therefore, practical key players must understand the differences and evaluate the dependencies and impacts. It is further crucial that these domains work together to prevent isolated concepts and misunderstandings.
In extension to the sustainable aspects mentioned in the introduction, companies and countries have to work together to steer in the direction of carbon neutrality and to achieve the agreed targets in the Paris Agreement (Caravella, Costantini, and Crespi, 2021). Data ecosystems and current research projects such as the IDS or GAIA-X help with this challenge in a practical context by creating systems built on data sovereign principles that follow the strategies and regulations of digital and technological sovereignty. Building on the results of this work, delimitating the term helps to strengthen trust between different parties through the internalization of data-sharing principles needed to accelerate innovation to solve sustainable challenges.

6.3 Limitations and Future Research

Despite careful work and evaluation, this study and the results have some limitations and points of contact for future research, discussed in the following.

Firstly, the search term selection only focuses on the three concepts: data, digital and technological sovereignty. Research has shown several papers discussing similar ideas, such as data protection, ownership, and maintaining usage or access control. One example is shown in the paper from Gates and Slonim (2003), addressing privacy, control, and data aspects without mentioning any sovereignty term. In this case, research might relate to data sovereignty without using the term. Therefore, further research is essential to understand better the relationship between the concepts of data sovereignty and data protection, data ownership, or similar terms.
Secondly, Figure 4 depicts the original distribution of the literature based on the main authors' institution. Notably, a large part of the publications is rooted in Europe, with an apparent underrepresentation of Africa, Australia, and South America ($<= 1\%$). Future research needs to evaluate the reasons and implications of the distribution and possible effects on transnational activities, like impacts on software implementations used in different regions.
Thirdly, this research's results do not clearly show, that the motivation for more sovereignty often lies in achieving more sustainability. Since the implementation of data sovereignty can promote more data sharing, sustainability goals can be achieved because organizations share their data for a greater common good to achieve more climate protection (DSSC, 2023). However, this study's focus did not cover the link between sustainability goals and the implementation of one of the sovereignty terms in detail and therefore needed to be discussed in future research.
Lastly, we argued that technological and digital sovereignty influence data sovereignty in IS research, as shown by several examples like national or international regulations that protect individual or organizational data. It is still unsettled if data sovereign models or systems can be created, even if none of the other two concepts are implemented. Future research has to analyze each concept's realization and how this encourages or prevents others.

7 Conclusion

Our literature has pointed out the delimitation of data sovereignty from digital and technological sovereignty and aims to contribute to a better understanding and coordinated usage of the concepts. Concluding, it is recommendable for IS research not to use data, digital, and technological sovereignty as if they were interchangeable concepts – they do not mean the same. Instead, the results of the RQ can be summarized as follows:
The concept of data sovereignty is embedded in IS research and used in the context of control over data on an individual or organizational level. Instead, technological sovereignty is essential in the political discourse with mostly international targets. This concept focuses on the usage and reduced dependencies of resources from other nations and trade areas and the preservation of solid relations. Therefore, the target of digital sovereignty lies in the political and economic realm. It refers to the digital literacy of a population and the level of development of an organization's digital features with control over infrastructures and aspects of interoperability.
As shown in the discussion, the delimitation of data sovereignty from adjacent fields, such as digital sovereignty and technological sovereignty, is essential to give future research and software architecture development a fundamental groundwork for using the terminologies with unanswered questions. Moreover, as pointed out in the study, data sovereignty cannot only be viewed from an IS research perspective since it is interwoven with other domains that influence it and contribute to the developments in the digital economy.

Acknowledgments

This work was partially funded by the "Silicon Economy Logistics Ecosystem" project. The project "Silicon Economy Logistics Ecosystem" is funded by the German Federal Ministry of Transport and Digital Infrastructure.

Appendix

No.	Source (Author & Year)	*Data Sov.*	*Digital Sov.*	*Techno. Sov.*
1	Adonis (2019)		x	
2	ASD (2020)			x
3	Aydin and Bensghir (2019)	x		
4	Banse (2021)	x		
5	Bauer et al. (2019)	x		
6	Bendiek and Neyer (2020)		x	
7	Braud et al. (2021)		x	
8	Calzada (2021a)	x		
9	Calzada (2021b)			x
10	Caravella, Costantini, and Crespi (2021)			x
11	Cattaruzza et al. (2016)		x	
12	Chapdelaine and McLeod Rogers (2021)	x	x	
13	Chen et al. (2020)	x		
14	Christakis (2020)		x	
15	Corbett and Cochrane (2020)	x		
16	Couture and Toupin (2019)	x	x	x
17	Crespi et al. (2021)		x	x
18	Cuno et al. (2019)	x		
19	Dabrock (2020)	x		
20	Diesen (2021)			x
21	Edler et al. (2020)			x
22	Edler et al. (2021)			x
23	Esposito, Castiglione, and Choo (2016)	x		
24	Esposito et al. (2019)	x		
25	European Commission (2020)			x
26	Filippi and McCarthy (2012)	x		
27	Floridi (2020)		x	
28	Friedrichsen and Bisa (2016)		x	
29	German Ethics Council (2017)	x		
30	Grant (1983)			x
31	Gupta, Lanteigne, and Kingsley (2020)	x		
32	Hallinan (2022)		x	
33	Hartsch et al. (2021)	x		
34	Hong and Kim (2020)	x		
35	Hummel et al. (2018)	x		
36	Hummel et al. (2021)	x	x	
37	Irion (2012)	x		
38	Janardhanan and Mas-Machuca (2022)		x	x
39	Jarke, Otto, and Ram (2019)	x		
40	Kagermann, Streibich, and Suder (2021)		x	
41	Komaitis (2021)		x	
42	Kukkola (2018)		x	
43	Kushwaha, Roguski, and Watson (2020)	x	x	x
44	Lauf et al. (2021)	x		
45	Lian (2021)	x		
46	Litvinenko (2021)		x	
47	Lynch (2020)			x
48	Mannhardt et al. (2019)	x		
49	March and Schieferdecker (2021)			x
50	Mark (2019)	x		
51	Martens and Zscheischler (2022)	x		
52	Maurer et al. (2015)			x
53	Mawere and van Stam (2020)	x		x
54	Merkel (2019)		x	
55	Micheli et al. (2020)	x		
56	Mooy (2017)	x		
57	Munoz-Arcentales et al. (2019)	x		
58	Nagel and Lycklama (2021)	x		
59	Nast et al. (2020)	x		
60	Nugraha, Kautsarina, and Sastrosubroto (2015)	x		
61	Otto (2019)	x		
62	Otto and Burmann (2021)	x		
63	Pedreira, Barros, and Pinto (2021)	x	x	
64	Peterson, Gondree, and Beverly (2011)	x		
65	Plateaux et al. (2013)	x		
66	Pohle and Thiel (2020)		x	
67	Polatin-Reuben and Wright (2014)	x		
68	Posch (2017)		x	
69	Qarawlus et al. (2021)	x		
70	Redeker et al. (2020)	x		
71	Ruohonen (2021)		x	
72	Ruparelia (2016)	x		
73	Sarabia-Jacome et al. (2019)	x		
74	Schleicher et al. (2011)	x		
75	Singi et al. (2020)	x		
76	Tan, Chi, and Lam (2022)	x	x	
77	Taylor (2020)	x		
78	Vaile (2014)	x		
79	von der Leyen (2020)			x
80	Zieglmeier and Pretschner (2021)	x		
81	Zrenner et al. (2019)	x		
∑	*81 publications*	*51*	*24*	*17*

Table 1. Final Literature Set.

References

4D Data Centres (2018). *The state of the UK server room*. URL: https://cdn2.hubspot.net/hubfs/6750926/4D_Data_Centres_December2019/Pdf/4D_DC_UK_Server_Room_Whitepaper.pdf (visited on Mar. 15, 2023).

Adonis, A. A. (2019). "Critical Engagement on Digital Sovereignty in International Relations: Actor Transformation and Global Hierarchy." *Global: Jurnal Politik Internasional* 21 (2), 262–282. ISSN: 1411-5492. DOI: 10.7454/global.v21i2.412.

AIT (2022). *Data Sovereignty for a Sustainable, Competitive Soviety*. Ed. by AIT Austrian Institute of Technology. URL: https://www.ait.ac.at/news-events/single-view/detail/7373?cHash=4391e19a3b1a4ad72aecb5102418e5c3 (visited on Mar. 15, 2023).

ASD (2020). *Industry considerations on Technological Sovereignty*. Ed. by AeroSpace and Defence Industries Association of Europe. Brussels. URL: https://www.asd-europe.org/industry-considerations-on-technological-sovereignty-concept-paper (visited on Mar. 15, 2023).

Asswad, J. and J. Marx Gómez (2021). "Data Ownership: A Survey." *Information* 12 (11), 1–32. DOI: 10.3390/info12110465.

Aydin, A. and T. K. Bensghir (2019). "Digital Data Sovereignty: Towards a Conceptual Framework." In: *2019 1st International Informatics and Software Engineering Conference (UBMYK)*. IEEE, pp. 1–6. ISBN: 978-1-7281-3992-0. DOI: 10.1109/UBMYK48245.2019.8965469.

Baezner, M. and P. Robin (2018). *Cyber Sovereignty and Data Sovereignty*. DOI: 10.3929/ethz-b-000314613.

Bandara, W., E. Furtmueller, E. Gorbacheva, S. Miskon, and J. Beekhuyzen (2015). "Achieving Rigor in Literature Reviews: Insights from Qualitative Data Analysis and Tool-Support." *Communications of the Association for Information Systems* 37, 154–204. DOI: 10.17705/1CAIS.03708.

Banse, C. (2021). "Data Sovereignty in the Cloud - Wishful Thinking or Reality?" In: *Proceedings of the 2021 on Cloud Computing Security Workshop*. Ed. by Y. Zhang and M. van Dijk. New York, USA: ACM, pp. 153–154. ISBN: 9781450386531. DOI: 10.1145/3474123.3486792.

Bauer, J., R. Helmke, A. Bothe, and N. Aschenbruck (2019). "CAN't track us: Adaptable privacy for ISOBUS controller area networks." *Computer Standards & Interfaces* 66, 103344. ISSN: 0920-5489. DOI: 10.1016/j.csi.2019.04.003.

Bendiek, A. and J. Neyer (2020). "Europas digitale Souveränität. Bedingungen und Herausforderungen internationaler politischer Handlungsfähigkeit." In: *Demokratietheorie im Zeitalter der Frühdigitalisierung*. Ed. by M. Oswald and I. Borucki. Wiesbaden and Heidelberg: Springer VS, pp. 103–125. ISBN: 978-3-658-30996-1. DOI: 10.1007/978-3-658-30997-8_6.

Benzies, K. M., S. Premji, K. A. Hayden, and K. Serrett (2006). "State-of-the-evidence reviews: advantages and challenges of including grey literature." *Worldviews on evidence-based nursing* 3 (2), 55–61. ISSN: 1545-102X. DOI: 10.1111/j.1741-6787.2006.00051.x.

Bodin, J. (1577). *Les six liures de la republique*.

Braud, A., G. Fromentoux, B. Radier, and O. Le Grand (2021). "The Road to European Digital Sovereignty with Gaia-X and IDSA." *IEEE Network* 35 (2), 4–5. ISSN: 0890-8044. DOI: 10.1109/MNET.2021.9387709.

Calzada, I. (2021a). "Data Co-Operatives through Data Sovereignty." *Smart Cities* 4 (3), 1158–1172. DOI: 10.3390/smartcities4030062.

Calzada, I. (2021b). "Epilogue. RESETTING smart city citizenship: Amidst the post-COVID-19 hyperconnected-virialised societies." In: *Smart City Citizenship*. Elsevier, pp. 235–244. ISBN: 9780128153000. DOI: 10.1016/B978-0-12-815300-0.09987-1.

Caravella, S., V. Costantini, and F. Crespi (2021). "Mission-Oriented Policies and Technological Sovereignty: The Case of Climate Mitigation Technologies." *Energies* 14 (20), 6854. DOI: 10.3390/en14206854.

Cattaruzza, A., D. Danet, S. Taillat, and A. Laudrain (2016). "Sovereignty in cyberspace: Balkanization or democratization." In: *2016 International Conference on Cyber Conflict (CyCon U.S.)* IEEE, pp. 1–9. ISBN: 978-1-5090-5258-5. DOI: 10.1109/CYCONUS.2016.7836628.

Chapdelaine, P. and J. McLeod Rogers (2021). "Contested Sovereignties: States, Media Platforms, Peoples, and the Regulation of Media Content and Big Data in the Networked Society." *Laws* 10 (3), 66. DOI: 10.3390/laws10030066.

Chen, Y., S. Chen, J. Liang, L. W. Feagan, W. Han, S. Huang, and X. S. Wang (2020). "Decentralized data access control over consortium blockchains." *Information Systems* 94, 101590. ISSN: 0306-4379. DOI: 10.1016/j.is.2020.101590.

Christakis, T. (2020). "'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy." *SSRN Electronic Journal*, 1–103. DOI: 10.2139/ssrn.3748098.

Corbett, J. and L. Cochrane (2020). "Geospatial Web, Participatory." In: *International Encyclopedia of Human Geography*. Elsevier, pp. 131–136. ISBN: 9780081022962. DOI: 10.1016/B978-0-08-102295-5.10604-3.

Couture, S. and S. Toupin (2019). "What does the notion of "sovereignty" mean when referring to the digital?" *New Media & Society* 21 (10), 2305–2322. ISSN: 1461-4448. DOI: 10.1177/1461444819865984.

Crespi, F., S. Caravella, M. Menghini, and C. Salvatori (2021). "European Technological Sovereignty: An Emerging Framework for Policy Strategy." *Inter economics* 56 (6), 348–354. ISSN: 0020-5346. DOI: 10.1007/s10272-021-1013-6.

Cuno, S., L. Bruns, N. Tcholtchev, P. Lämmel, and I. Schieferdecker (2019). "Data Governance and Sovereignty in Urban Data Spaces Based on Standardized ICT Reference Architectures." *Data* 4 (1), 16. DOI: 10.3390/data4010016.

Dabrock, P. (2020). "How to Put the Data Subject's Sovereignty into Practice. Ethical Considerations and Governance Perspectives." In: *Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society*. Ed. by A. Markham, J. Powles, T. Walsh, and A. L. Washington. New York, USA: ACM, pp. 1–2. ISBN: 9781450371100. DOI: 10.1145/3375627.3377142.

Diesen, G. (2021). *Great Power Politics in the Fourth Industrial Revolution: The Geoeconomics of Technological Sovereignty*. First edition. London: I. B. Tauris & Company Limited. ISBN: 978-0-7556-0701-3. DOI: 10.5040/9780755607037.

DSSC (2023). *Starter Kit for Data Space Designers*. Ed. by Data Spaces Support Centre. URL: https://dssc.eu/download/802/ (visited on Mar. 23, 2023).

Edler, J., K. Blind, R. Frietsch, S. Kimpeler, H. Kroll, C. Lerch, T. Reiss, F. Roth, T. Schubert, J. Schuler, and R. Walz (2020). *Technology sovereignty: From demand to concept*. Ed. by Fraunhofer ISI. Karlsruhe, Germany. URL: https://publica.fraunhofer.de/dokumente/N-599757.html (visited on Mar. 15, 2023).

Edler, J., K. Blind, H. Kroll, and T. Schubert (2021). *Technology Sovereignty as an Emerging Frame for Innovation Policy – Defining Rationales, Ends and Means*. Ed. by Fraunhofer ISI. Karlsruhe, Germany. URL: https://publica.fraunhofer.de/dokumente/N-638343.html (visited on Mar. 15, 2023).

Esposito, C., A. Castiglione, and K.-K. R. Choo (2016). "Encryption-Based Solution for Data Sovereignty in Federated Clouds." *IEEE Cloud Computing* 3 (1), 12–17. DOI: 10.1109/MCC.2016.18.

Esposito, C., A. Castiglione, F. Frattini, M. Cinque, Y. Yang, and K.-K. R. Choo (2019). "On Data Sovereignty in Cloud-Based Computation Offloading for Smart Cities Applications." *IEEE Internet of Things Journal* 6 (3), 4521–4535. DOI: 10.1109/JIOT.2018.2886410.

European Commission (2020). *Shaping Europe's Digital Future*. Ed. by European Union. DOI: 10.2759/091014.

Filippi, P. de and S. McCarthy (2012). "Cloud Computing: Centralization and Data Sovereignty." *European Journal of Law and Technology* 3 (2), 1–18. URL: https://ssrn.com/abstract=2167372 (visited on Mar. 15, 2023).

Floridi, L. (2020). "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU." *Philosophy & technology* 33 (3), 369–378. ISSN: 2210-5433. DOI: 10.1007/s13347-020-00423-6.

Friedrichsen, M. and P.-J. Bisa, eds. (2016). *Digitale Souveränität: Vertrauen in der Netzwerkgesellschaft*. Wiesbaden: Springer VS. ISBN: 978-3-658-07349-7.

Garousi, V., M. Felderer, and M. V. Mäntylä (2019). "Guidelines for including grey literature and conducting multivocal literature reviews in software engineering." *Information and Software Technology* 106, 101–121. ISSN: 0950-5849. DOI: 10.1016/j.infsof.2018.09.006.

Gates, C. and J. Slonim (2003). "Owner-controlled information." In: *Proceedings of the 2003 workshop on New security paradigms - NSPW '03*. Ed. by O. S. Saydjari, S. Foley, R. Sekar, C. F. Hempelmann, and V. Raskin. New York, USA: ACM Press, pp. 103–111. ISBN: 1581138806. DOI: 10.1145/986655.986670.

German Ethics Council (2017). *Big Data and Health – Data Sovereignty as the Shaping of Informational Freedom: Executive Summary & Recommendations*. Berlin. URL: https://www.ethikrat.org/en/publications/publication-details/?tx_wwt3shop_detail%5Bproduct%5D=4&tx_wwt3shop_detail%5Baction%5D=index&tx_wwt3shop_detail%5Bcontroller%5D=Products&cHash=7bb9aadb656b877f9dbd49a61e39df2f (visited on Mar. 15, 2023).

Grant, P. (1983). "Technological Sovereignty: Forgotten Factor in the 'Hi-Tech' Razzamatazz." *Prometheus* 1 (2), 239–270. ISSN: 0810-9028. DOI: 10.1080/08109028308628930.

Gupta, A., C. Lanteigne, and S. Kingsley (2020). *SECure: A Social and Environmental Certificate for AI Systems*. DOI: 10.48550/arXiv.2006.06217.

Hallinan, D. (2022). *Data Protection and Privacy, Volume 14: Enforcing Rights in a Changing World*. Computers, Privacy and Data Protection Ser. London: Bloomsbury Publishing Plc. ISBN: 9781509954513.

Hartsch, F., J. Kemmerer, E. R. Labelle, D. Jaeger, and T. Wagner (2021). "Integration of Harvester Production Data in German Wood Supply Chains: Legal, Social and Economic Requirements." *Forests* 12 (4), 460. DOI: 10.3390/f12040460.

Hong, S. and H. Kim (2020). "VaultPoint: A Blockchain-Based SSI Model that Complies with OAuth 2.0." *Electronics* 9 (8), 1231. DOI: 10.3390/electronics9081231.

Hummel, P., M. Braun, S. Augsberg, and P. Dabrock (2018). "Sovereignty and data sharing." *ITU Journal: ICT Discoveries* 1 (2). ISSN: 2616-8375.

Hummel, P., M. Braun, M. Tretter, and P. Dabrock (2021). "Data sovereignty: A review." *Big Data & Society* 8 (1), 1–17. ISSN: 2053-9517. DOI: 10.1177/2053951720982012.

Irion, K. (2012). "Government Cloud Computing and National Data Sovereignty." *Policy & Internet* 4 (3-4), 40–71. ISSN: 1944-2866. DOI: 10.1002/poi3.10.

Janardhanan, S. and C. Mas-Machuca (2022). "Modeling and Evaluation of a Data Center Sovereignty." In: *2022 18th International Conference on the Design of Reliable Communication Networks (DRCN)*. IEEE, pp. 1–8. ISBN: 978-1-6654-0987-2. DOI: 10.1109/DRCN53993.2022.9758037.

Jarke, M., B. Otto, and S. Ram (2019). "Data Sovereignty and Data Space Ecosystems." *Business & Information Systems Engineering* 61 (5), 549–550. ISSN: 2363-7005. DOI: 10.1007/s12599-019-00614-2.

Kagermann, H., K.-H. Streibich, and K. Suder (2021). *Digital Sovereignty: Status Quo and Perspectives*. acatech Impuls. Munich: acatech - National Academy of Science and Engineering. ISBN: 978-3-96834-011-1.

Komaitis, K. (2021). "Europe's ambition for digital sovereignty must not undermine the Internet's values." *Computer Fraud & Security* 2021 (1), 11–13. ISSN: 1361-3723. DOI: 10.1016/S1361-3723(21)00008-7.

Kuhrmann, M., D. M. Fernández, and M. Daneva (2017). "On the pragmatic design of literature studies in software engineering: an experience-based guideline." *Empirical Software Engineering* 22 (6), 2852–2891. ISSN: 1382-3256. DOI: 10.1007/s10664-016-9492-y.

Kukkola, J. (2018). "Civilian and military information infrastructure and the control of the Russian segment of Internet." In: *2018 International Conference on Military Communications and Information Systems (ICMCIS)*. IEEE, pp. 1–8. ISBN: 978-1-5386-4559-8. DOI: 10.1109/ICMCIS.2018.8398700.

Kushwaha, N., P. Roguski, and B. W. Watson (2020). "Up in the Air: Ensuring Government Data Sovereignty in the Cloud." In: *2020 12th International Conference on Cyber Conflict (CyCon)*. IEEE, pp. 43–61. ISBN: 9789-949-9904-7-4. DOI: 10.23919/CyCon49761.2020.9131718.

Lauf, F., S. Scheider, S. Meister, M. Radic, P. Herrmann, M. Schulze, A. T. Nemat, S. J. Becker, M. Rebbert, C. Abate, R. Konrad, J. Bartsch, T. Dehling, and A. Sunyaev (2021). *Data Sovereignty and Data Economy—Two Repulsive Forces?* Ed. by Fraunhofer Institute for Software and Systems Engineering ISST. Dortmund. DOI: 10.24406/ISST-N-634865.

Lian, Y. (2021). *Data Rights Law 3.0*. Peter Lang UK. ISBN: 9781789978384.

Litvinenko, A. (2021). "Re-Defining Borders Online: Russia's Strategic Narrative on Internet Sovereignty." *Media and Communication* 9 (4), 5–15. DOI: 10.17645/mac.v9i4.4292.

Lynch, C. R. (2020). "Contesting Digital Futures: Urban Politics, Alternative Economies, and the Movement for Technological Sovereignty in Barcelona." *Antipode* 52 (3), 660–680. ISSN: 0066-4812. DOI: 10.1111/anti.12522.

Mannhardt, F., A. Koschmider, N. Baracaldo, M. Weidlich, and J. Michael (2019). "Privacy-Preserving Process Mining - Differential Privacy for Event Logs." *Business & Information Systems Engineering* 61 (5), 595–614. ISSN: 2363-7005. DOI: 10.1007/s12599-019-00613-3.

March, C. and I. Schieferdecker (2021). "Technological Sovereignty as Ability, Not Autarky." *SSRN Electronic Journal*, 1–39. DOI: 10.2139/ssrn.3872378.

Mark, R. (2019). "Ethics of Public Use of AI and Big Data." *The ORBIT Journal* 2 (2), 1–33. ISSN: 2515-8562. DOI: 10.29297/orbit.v2i1.101.

Martens, K. and J. Zscheischler (2022). "The Digital Transformation of the Agricultural Value Chain: Discourses on Opportunities, Challenges and Controversial Perspectives on Governance Approaches." *Sustainability* 14 (7). DOI: 10.3390/su14073905.

Maurer, T., I. Skierka, R. Morgus, and M. Hohmann (2015). "Technological sovereignty: Missing the point?" In: *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*. IEEE, pp. 53–68. ISBN: 978-9-9499-5442-1. DOI: 10.1109/CYCON.2015.7158468.

Mawere, M. and G. van Stam (2020). "Data Sovereignty: A Perspective From Zimbabwe." In: *12th ACM Conference on Web Science Companion*. New York, USA: ACM, pp. 13–19. ISBN: 9781450379946. DOI: 10.1145/3394332.3402823.

Merkel, A. (2019). *Speech by Federal Chancellor Dr Angela Merkel opening the 14th Annual Meeting of the Internet Governance Forum in Berlin on 26 November 2019*. Berlin. URL: https://www.bundeskanzler.de/bk-en/news/speech-by-federal-chancellor-dr-angela-merkel-opening-the-14th-annual-meeting-of-the-internet-governance-forum-in-berlin-on-26-november-2019-1701494 (visited on Mar. 15, 2023).

Micheli, M., M. Ponti, M. Craglia, and A. Berti Suman (2020). "Emerging models of data governance in the age of datafication." *Big Data & Society* 7 (2), 1–15. ISSN: 2053-9517. DOI: 10.1177/2053951720948087.

Mooy, M. de (2017). *Rethinking Privacy Self-Management and Data Sovereignty in the Age of Big Data*. Ed. by Bertelsmann Foundation. DOI: 10.11586/2017009.

Munoz-Arcentales, A., S. López-Pernas, A. Pozo, Á. Alonso, J. Salvachúa, and G. Huecas (2019). "An Architecture for Providing Data Usage and Access Control in Data Sharing Ecosystems." *Procedia Computer Science* 160, 590–597. ISSN: 1877-0509. DOI: 10.1016/j.procs.2019.11.042.

Nagel, L. and D. Lycklama (2021). *Design Principles for Data Spaces - Position Paper*. Ed. by International Data Spaces Association. DOI: 10.5281/ZENODO.5105744.

Nast, M., B. Rother, F. Golatowski, D. Timmermann, J. Leveling, C. Olms, and C. Nissen (2020). "Work-in-Progress: Towards an International Data Spaces Connector for the Internet of Things." In: *2020 16th IEEE International Conference on Factory Communication Systems (WFCS)*. IEEE, pp. 1–4. ISBN: 978-1-7281-5297-4. DOI: 10.1109/WFCS47810.2020.9114503.

Nugraha, Y., Kautsarina, and A. S. Sastrosubroto (2015). "Towards data sovereignty in cyberspace." In: *2015 3rd International Conference on Information and Communication Technology (ICoICT)*. IEEE, pp. 465–471. DOI: 10.1109/icoict.2015.7231469.

Otto, B. (2019). *Interview with Reinhold Achatz on "Data Sovereignty and Data Ecosystems"*. DOI: 10.1007/s12599-019-00609-z.

Otto, B. and A. Burmann (2021). "Europäische Dateninfrastrukturen." *Informatik Spektrum* 44 (4), 283–291. ISSN: 0170-6012. DOI: 10.1007/s00287-021-01386-4.

Otto, B., S. Steinbuss, A. Teuscher, and S. Lohmann (2019). *IDS Reference Architecture Model*. Ed. by International Data Spaces Association. DOI: 10.5281/ZENODO.5105529.

Pedreira, V., D. Barros, and P. Pinto (2021). "A Review of Attacks, Vulnerabilities, and Defenses in Industry 4.0 with New Challenges on Data Sovereignty Ahead." *Sensors* 21 (15), 5189. DOI: 10.3390/s21155189.

Perarnaud, C. and R. Fanni (2022). *The EU Data Act: Towards a new European data revolution?* URL: https://ideas.repec.org/p/eps/cepswp/35693.html (visited on Mar. 15, 2023).

Peterson, Z. N. J., M. Gondree, and R. Beverly (2011). "A Position Paper on Data Sovereignty: The Importance of Geolocating Data in the Cloud." In: *Proceedings of the 3rd USENIX Conference on Hot Topics in Cloud Computing*. Ed. by I. Stoica and J. Wilkes. USENIX Association, pp. 1–5. URL: https://dl.acm.org/doi/10.5555/2170444.2170453 (visited on Mar. 15, 2023).

Plateaux, A., P. Lacharme, C. Rosenberger, and K. Murty (2013). "A contactless e-health information system with privacy." In: *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*. IEEE, pp. 1660–1665. ISBN: 978-1-4673-2480-9. DOI: 10.1109/IWCMC.2013.6583805.

Pohle, J. and T. Thiel (2020). "Digital sovereignty." *Internet Policy Review* 9 (4), 1–19. ISSN: 2197-6775. DOI: 10.14763/2020.4.1532.

Polatin-Reuben, D. and J. Wright (2014). "An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet." *4th USENIX Workshop on Free and Open Communications on the Internet*, 1–10. URL: https://www.usenix.org/conference/foci14/workshop-program/presentation/polatin-reuben (visited on Mar. 15, 2023).

Posch, R. (2017). "Digital Sovereignty and IT-Security for a Prosperous Society." In: *Informatics in the Future*. Ed. by H. Werthner and F. van Harmelen. Cham: Springer International Publishing, pp. 77–86. ISBN: 978-3-319-55734-2. DOI: 10.1007/978-3-319-55735-9_7.

Qarawlus, H., M. Hellmeier, J. Pieperbeck, R. Quensel, S. Biehs, and M. Peschke (2021). "Sovereign Data Exchange in Cloud-Connected IoT using International Data Spaces." In: *2021 IEEE Cloud Summit (Cloud Summit)*. IEEE, pp. 13–18. ISBN: 978-1-6654-2582-7. DOI: 10.1109/IEEECloudSummit52029.2021.00010.

Redeker, M., S. Volgmann, F. Pethig, and J. Kalhoff (2020). "Towards Data Sovereignty of Asset Administration Shells across Value Added Chains." In: *2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)*. IEEE, pp. 1151–1154. ISBN: 978-1-7281-8956-7. DOI: 10.1109/ETFA46521.2020.9211955.

Ruohonen, J. (2021). "The Treachery of Images in the Digital Sovereignty Debate." *Minds and Machines* 31 (3), 439–456. ISSN: 0924-6495. DOI: 10.1007/s11023-021-09566-7.

Ruparelia, N. B. (2016). *Cloud computing*. The MIT Press essential knowledge series. Cambridge, Massachusetts and London, England: The MIT Press. ISBN: 9780262334129.

Sarabia-Jacome, D., I. Lacalle, C. E. Palau, and M. Esteve (2019). "Enabling Industrial Data Space Architecture for Seaport Scenario." In: *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*. IEEE, pp. 101–106. ISBN: 978-1-5386-4980-0. DOI: 10.1109/WF-IoT.2019.8767216.

Schleicher, D., C. Fehling, S. Grohe, F. Leymann, A. Nowak, P. Schneider, and D. Schumm (2011). "Compliance Domains: A Means to Model Data-Restrictions in Cloud Environments." In: *2011 IEEE 15th International Enterprise Distributed Object Computing Conference*. IEEE, pp. 257–266. ISBN: 978-1-4577-0362-1. DOI: 10.1109/EDOC.2011.22.

Singi, K., S. G. Choudhury, V. Kaulgud, R. J. C. Bose, S. Podder, and A. P. Burden (2020). "Data Sovereignty Governance Framework." In: *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*. New York, USA: ACM, pp. 303–306. ISBN: 9781450379632. DOI: 10.1145/3387940.3392212.

Tan, K.-L., C.-H. Chi, and K.-Y. Lam (2022). *Analysis of Digital Sovereignty and Identity: From Digitization to Digitalization*. arXiv. DOI: 10.48550/arXiv.2202.10069.

Taylor, J. and T. Kukutai, eds. (2016). *Indigenous data sovereignty: Toward an agenda*. Vol. no. 38. Research monograph / Centre for Aboriginal Economic Policy Research, College of Arts and Social Sciences, The Australian National University, Canberra. Acton, ACT, Australia: Australian National University Press. ISBN: 9781760460303.

Taylor, R. D. (2020). ""Data localization": The internet in the balance." *Telecommunications Policy* 44 (8), 102003. ISSN: 0308-5961. DOI: 10.1016/j.telpol.2020.102003.

Vadiati, N. (2022). "Alternatives to smart cities: A call for consideration of grassroots digital urbanism." *Digital Geography and Society* 3, 100030. ISSN: 2666-3783. DOI: 10.1016/j.diggeo.2022.100030.

Vaile, D. (2014). "The Cloud and data sovereignty after Snowden." *Australian Journal of Telecommunications and the Digital Economy* 2 (1), 1–59. ISSN: 2203-1693. DOI: 10.7790/ajtde.v2n1.31.

vom Brocke, J., A. Simons, B. Niehaves, B. Niehaves, K. Reimer, R. Plattfaut, and A. Cleven (2009). "Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process." *ECIS 2009 Proceedings*.

vom Brocke, J., A. Simons, K. Riemer, B. Niehaves, R. Plattfaut, and A. Cleven (2015). "Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research." *Communications of the Association for Information Systems* 37, 205–224. DOI: 10.17705/1CAIS.03709.

von der Leyen, U. (2020). *Shaping Europe's digital future: op-ed by Ursula von der Leyen, President of the European Commission*. Brussels. URL: https://ec.europa.eu/commission/presscorner/detail/en/ac_20_260 (visited on Mar. 15, 2023).

Webster, J. and R. T. Watson (2002). "Analyzing the Past to Prepare for the Future: Writing a Literature Review." *MIS Quarterly* 26 (2), xiii–xxiii. ISSN: 0276-7783.

Zieglmeier, V. and A. Pretschner (2021). *Trustworthy Transparency by Design*. DOI: 10.48550/arXiv.2103.10769.

Zrenner, J., F. O. Möller, C. Jung, A. Eitel, and B. Otto (2019). "Usage control architecture options for data sovereignty in business ecosystems." *Journal of Enterprise Information Management* 32 (3), 477–495. ISSN: 1741-0398. DOI: 10.1108/JEIM-03-2018-0058.