Electronic Markets (2024) 34:15
https://doi.org/10.1007/s12525-024-00693-4

FUNDAMENTALS

Data Sovereignty in Information Systems

Franziska von Scherenberg[1] · **Malte Hellmeier**[1] · **Boris Otto**[1,2]

Received: 27 January 2023 / Accepted: 12 January 2024

Abstract
Data has become a strategic asset for societal prosperity and economic competitiveness. There has long been an academic consensus that the value of data unfolds during its use. Consequently, many stakeholders have called for expanding the use and reuse of data, including the public and open variety, as well as that from private data providers. However, citizens and organizations want self-determination over their data use, that is, data sovereignty. This fundamentals paper applies a literature review to conceptualize the term in Information Systems (IS) research by summarizing current findings and definitions to add further structure to the field. It contributes to the current research streams by introducing a core conceptual model consisting of seven interacting core aspects, involving trust between data providers and consumers for data assets, supported by data infrastructure and contractual agreements on all data lifecycle stages. We evaluate and discuss this conceptual model through recent field examples and provide an overview of future research opportunities.

Keywords Data sovereignty · Information systems · Literature review · Conceptualization

JEL Classification L86 · M15

Introduction

Data assets are digital goods and the basis for all Information Systems (IS). They have become a strategic asset for societal prosperity and economic competitiveness. Accordingly, studying data as a concept is essential for further developments in IS research (Singi et al., 2020). According to recent estimations, data assets will grow in quantity and increase in importance in the upcoming years (Statista, 2022). More data sharing that further enables data-driven decision-making is one reason for this growth and increase (Munoz-Arcentales et al., 2019). However, those who share their data fear a loss of control and competitive disadvantage, which is why a data economy that protects the individual and organization's interests is vital (Lauf et al., 2021). In this context, data sovereignty becomes a success factor as its implementation strengthens actors to decide on the use of their data as an economic asset (Banse, 2021), thus paving the way to a digital space wherein providers and consumers can control all of their data actions.

Practically speaking, data sovereignty constitutes a key piece in building safe environments where data providers and consumers overcome trust issues while sharing data. Given the importance of handling data according to sovereignty principles, policymakers must ensure "fair data sharing practices" (European Commission, 2022, p. 26) and create secure frameworks. Legislations derived from the European Strategy for Data, such as the Data Governance Act (DGA) or the Data Act (DA), as well as the General Data Protection Regulation (GDPR) that came into force in 2016, regulate the data protection of different actors. They directly influence technological design in order to balance economic opportunities with society's interests in sharing and reusing data (Labadie et al., 2019). In addition, politicians, organizations, and other stakeholders recognize data sovereignty as essential for controlling the data of individuals and organizations; however, when referring to data

Responsible Editor: Christiane Lehrer

✉ Franziska von Scherenberg
franziska.von.scherenberg@isst.fraunhofer.de

Malte Hellmeier
malte.hellmeier@isst.fraunhofer.de

Boris Otto
boris.otto@isst.fraunhofer.de; boris.otto@tu-dortmund.de

[1] Fraunhofer ISST, Speicherstr. 6, 44147 Dortmund, Germany

[2] Chair for Industrial Information Management, TU Dortmund, Joseph-von-Fraunhofer-Str. 2-4, 44227 Dortmund, Germany

Published online: 27 February 2024

sovereignty, it is often unclear whether these actors share the same understanding of the concept.

A deeper understanding of how organizations and individuals technically implement control over data when sharing it is crucial for all research into digital self-determination and motivates the study of data sovereignty in IS. First, academia demands more alignment and less isolation in exploring the core aspects and relations of data sovereignty. Moreover, there is persistent terminological ambiguity in IS research, particularly in studies on indigenous people (Taylor & Kukutai, 2016), data sovereignty in the cloud (Irion, 2012), or data sovereignty of individuals and enterprises (Jarke et al., 2019), to name just a few examples. Additionally, holistic research on data sovereignty that observes the overall concept is either absent or fails to live up to the expectations of exploring the handling of data in a sovereign way within IS (Hummel et al., 2021; Kushwaha et al., 2020).

Moreover, former IS research has faced challenges, provided loose ends, or come to divergent conclusions. This is shown by different data sovereignty definitions with contrasting focuses on law (Docter & Fuchs, 2020), self-determination (Banse, 2021; Jarke et al., 2019; Nagel & Lycklama, 2021), data flows (Lauf et al., 2021), or informational freedom (German Ethics Council, 2017). Further, studies have focused on implementing data sovereignty without clarifying the concept's foundation (Opriel et al., 2021; Plattform Industrie 4.0, 2022). Other research has analyzed the impact of data sovereignty on data sharing without examining the concept itself (Azkan et al., 2022). Previous articles and studies have described sovereignty as a capability (Nagel & Lycklama, 2021) without proving a theoretical approach. This study aims to fill these gaps by analyzing the current state of research and developing a conceptual model that can help researchers and practitioners navigate this cluttered field so as to gain a mutual understanding of the concept.

This research is structured as follows: It begins by describing data sovereignty and contextualizing its background, as well as analyzing previous contributions in IS and adjacent domains from academia and practitioners. As described in detail in the appendix, a Multivocal Literature Review (MLR) is applied to developing a conceptual model (Fig. 1) that specifies the core aspects of data sovereignty (Table 2). It draws on agency theory to support a consistent understanding of the concept within the realm of IS, as well as to form a baseline for further analytical, exploratory, and design-oriented research. Using real-world examples, the proposed model illuminates all core aspects and explains their roles and relations. The paper concludes by discussing theoretical and practical implications while considering limitations and future research opportunities.

Background and related work

In the digital world, the concept of *sovereignty* describes forms of independence, control, and autonomy over digital infrastructures, technologies, data, and digital content

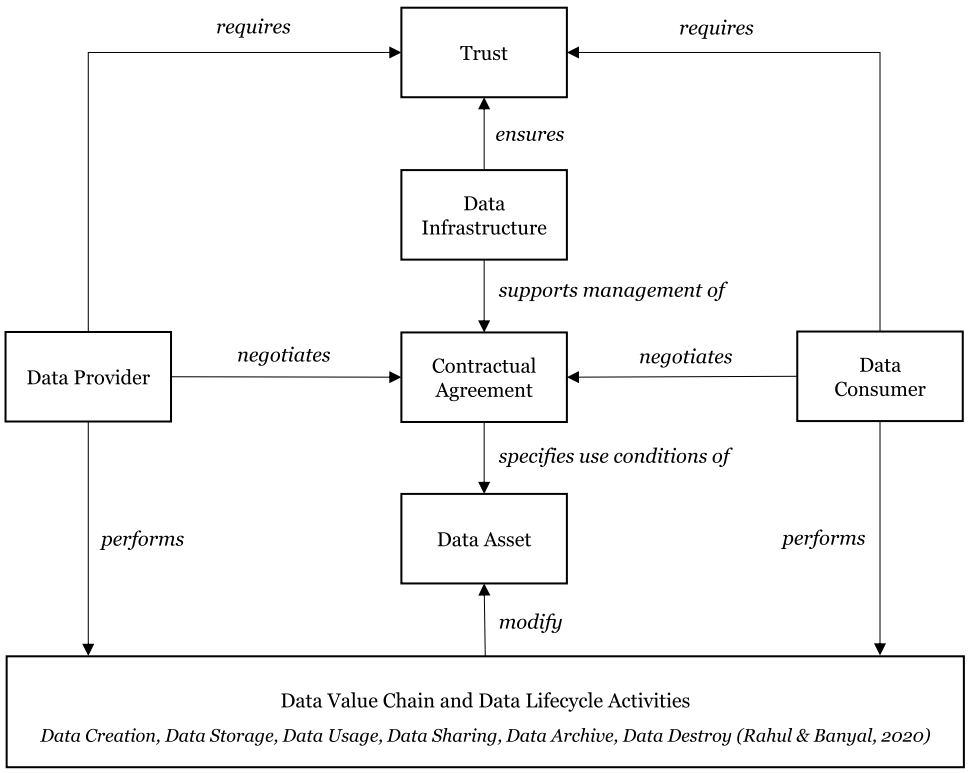

Fig. 1 Conceptualization of data sovereignty in IS

(Pohle & Thiel, 2020). Discussions of sovereignty with a technological focus began in the 1980s (Grant, 1983; Hinsley, 1986) when it extended to various forms and domains, such as technological-, digital-, data-, or cyber sovereignty (Hellmeier & von Scherenberg, 2023). *Data sovereignty* is a relatively new term used in decision-making and data ownership (Hummel et al., 2021). Over time, researchers have shaped its meaning, emphasizing its different nuances. Table 1 summarizes various data sovereignty definitions from different research domains to contextualize the concept.

Direct comparisons reveal different perspectives on the same term. For example, Polatin-Reuben and Wright (2014) mentioned a missing definition and shaped the concept on a national level, while both Jarke et al. (2019) and Nagel and Lycklama (2021) described it for individuals and enterprises. Other publications, such as the German Ethics Council (2017), included such technical aspects as big data, while Docter and Fuchs (2020) introduced the legal perspective. Research has often referred to the notion of digital *self-determination* that exceeds the perspective of data sovereignty as it considers not only one's data but also "data about oneself" (Verhulst, 2023, p. 8) and is related to protecting personal data and user consent. In contrast to data sovereignty, digital self-determination makes no distinctions between data and their actors but sees both as an entity (Verhulst, 2023).

Within IS, current discussions on data sovereignty are increasingly driven by regulations that balance data protection and use before, during, and after the sharing process, such as the European GDPR, the DGA (European Commission, 2020), and the DA (European Commission, 2022). However, control over data is not only a fundamental European principle. Such regulations as China's Personal Information Protection Law (PIPL) or the California Consumer Privacy Act (CCPA) show that it is also gaining increasing attention globally (Chander et al., 2021), as the global rise in data exploitation stems mainly from the market power of monopolistic US and Chinese organizations, thus explaining the increasing demand for new data governance models.

The technical implementation of data sovereignty can initiate beneficial consequences of data sharing since it enables organizations to find a solution for balancing data protection and use. These are, first, *cost sharing*, where actors save money and time when sharing their data under the prerequisites of data sovereignty; second, the *greater common good,* where organizations can, for example, be motivated to share data for the achievement of CO_2 targets; and third, *joint innovation,* which can only occur when actors work together, as most participants are unable to realize the application individually (Data Spaces Support Centre, 2023b). These examples show that value is not created by one player, but

Table 1 Collection of data sovereignty definitions

Authors	Definition	Research domain
Polatin-Reuben and Wright (2014, p. 1)	"The term 'data sovereignty', while lacking a firm definition, refers to a spectrum of approaches adopted by different states to control data generated in or passing through national internet infrastructure. It can be understood as a subset of cyber sovereignty, defined as the subjugation of the cyber domain to local jurisdictions."	IS
German Ethics Council (2017, p. 30)	"Data sovereignty, understood as the responsible shaping of informational freedom, in a manner appropriate to the risks and opportunities presented by big data, is the central ethical and legal goal in confronting the challenges and opportunities presented by big data."	Ethics/Humanities and Social Sciences
Jarke et al. (2019, p. 550)	"Data sovereignty refers to the self-determination of individuals and organizations with regard to the use of their data."	Computer Science
Sarabia-Jacome et al. (2019, p. 101)	"Consequently, the data sovereignty concept arises, which is defined as the ability of the data owner to decide itself how to share and use its data."	Electrical and Electronics Engineers Science
Docter and Fuchs (2020, p. 256)	"Data sovereignty is the concept that data is subject to laws and regulations of a particular nation."	IS
Hong and Kim (2020, p. 19)	"[...] data sovereignty, which refers to the right to use and control one's own information."	Computer Science
Lauf et al. (2021, p. 9)	"Our understanding of data sovereignty is the ability to formulate self-defined data-usage rules, influence and trace the data/information flows while being free in the decision of (not) sharing data and migrating data whenever and wherever it is desirable."	IS
Banse (2021, p. 10)	"Self-determination how, when and at what price others (across the value chain) may use my data"	Computer Science
Nagel and Lycklama (2021, p. 27)	"Data sovereignty is the capability of a natural person or corporate entity for exclusive self-determination with regard to its economic data goods."	IS

Table 2 Specification of the core conceptual data sovereignty aspects and relations

Core aspects	Specification
Data asset	An asset over which control is to be retained. It includes various possibilities, from files over complete batches, databases, or data warehouses to ideas and technologies. Such data assets must be controlled against their access and usage (Munoz-Arcentales et al., 2019).
Data provider	A natural person, company, or organization that has been given the right to control the data asset (Gil et al., 2020; Zrenner et al., 2019).
Data consumer	A natural person, company, or organization interested in using, creating, deleting, or sharing data assets owned or controlled by a data provider (Gil et al., 2020; Zrenner et al., 2019).
Contractual agreement	An agreement, signed by at least the data provider and connected to the data asset, determines their access and usage. The agreement is based on a previously negotiated contract, which can be verbal, written, or digital (Jarke et al., 2019).
Data value chain and data lifecycle activities	A cluster of all activities performed on the data asset throughout its lifecycle, from data creation to storage, analysis, sharing, and deletion (Curry, 2016; Rahul & Banyal, 2020).
Data infrastructure	A system or concept reviewing, documenting, and executing the rules of the contract agreement in the form of policy enforcement (Nagel & Lycklama, 2021), often included in current IT architectures (Hummel et al., 2021) as a data infrastructure (Munoz-Arcentales et al., 2019).
Trust	A fundamental core component for data sovereignty. On the one hand, it is required by all players who want to perform data value chain activities on a data asset (Peterson et al., 2011). On the other hand, the infrastructure helps with its amplification (Nagel & Lycklama, 2021).
Relations	**Specification**
Data provider and data consumer require trust	Trust is always required by all stakeholders as a baseline (Nagel & Lycklama, 2021).
Data infrastructure ensures trust	A manual or technical infrastructure helps ensure trust (Munoz-Arcentales et al., 2019), for example, through enforcement mechanisms.
Data provider and data consumer negotiate contract agreements	Data providers and consumers have to negotiate a contract to create an agreement that specifies the use conditions of the data asset (Zrenner et al., 2019).
Data infrastructure supports management of contractual agreement	A manual or technical infrastructure supports the management of contract agreements through validation techniques (Munoz-Arcentales et al., 2019).
Contractual agreement specifies use conditions of data asset	A contract agreement specifies the use conditions of the data asset, for example, through policies (Zrenner et al., 2019).
Data provider and data consumer perform data value chain and data lifecycle activities	Data providers or consumers with access to the data asset perform data value chain and data lifecycle activities (Otto et al., 2022).
Data value chain and data lifecycle activities modify data asset	A data asset can reach different statuses and versions because it is modified by data value chain activities (Curry, 2016; Rahul & Banyal, 2020).

through various actors' combinations and data enrichment in *data ecosystems* (Gelhaar et al., 2021).

The *ecosystem* concept originally stems from ecological science and draws on the attention of living organisms that co-exist in a healthy environment (Chapin et al., 2011). Ecosystems and, in this regard, *data ecosystems* do not function with central governance but rather work in balance. They can be open or closed (Oliveira & Lóscio, 2018), and while open data ecosystems are free for everyone to join, the closed variety often enforces technical or legal entry barriers (Capiello et al., 2020; Janssen et al., 2012; van den Homberg & Susha, 2018). Actors in data ecosystems depend on and benefit from each other in equilibrium, without one being dominant. As such, all actors should be equipped with an instrument to control their own data without being controlled by one central instance to create a trusted environment. Consequently, implementing data sovereignty is an essential part of this (Gelhaar et al., 2021; Otto et al., 2022).

Conceptualizing data sovereignty in IS research

This chapter proposes a data sovereignty conceptual model consisting of core conceptual aspects and relations. Conceptual models are critical for simplifying and abstracting

reality, as well as helping researchers and practitioners to understand, organize, and communicate complex or novel concepts (Houy et al., 2012). As described in the appendix, the conceptual model was developed by consulting the IS data sovereignty literature in Tables 1, 2, and Table S1. It is grounded in the agency theory to ensure that the model can fully explain the concept and offer a basis for real-world application (Eisenhardt, 1989).

The core of this theory, developed during the 1960s and 1970s, is to analyze the relationship between two actors (Eisenhardt, 1989). Its underlying assumption is that these two actors pursue their objectives, which often differ, acting in their self-interest. In addition, it implies an information asymmetry between both actors. In order to avoid mistrust, control mechanisms are installed that lead to greater transparency (Eisenhardt, 1989). With the help of this theory, challenges in organizational relationships can be more effectively uncovered, and governance structures more deeply understood (Eisenhardt, 1989).

Through the lens of this theory, data sovereignty can be implemented as an instrument with the central objective of establishing more trust. As outlined in the theory's description, contractual agreements provide the necessary transparency on the actions of both actors (here, data providers and consumers). According to Eisenhardt (1989), this theory can be applied to buyer–supplier and other agency relationships and, therefore, is suited for relations in the context of data sharing that arises in open or closed data ecosystems. With the implementation of data sovereignty, actors have an instrument at hand that paves the way for a more balanced power structure and supports all parties in pursuing their objectives.

The presented conceptual model applies the concept of data sovereignty in IS research, supporting both researchers and practitioners to develop a holistic understanding of the concept and serves to guide those (i.e., practitioners) who seek to implement data sovereignty technically. It aims for a completeness that has, as yet, not been provided by existing IS literature and definitions (see Table 1). In addition, this conceptual model helps all stakeholders better understand and communicate the concept of data sovereignty.

The seven core aspects referenced in Table 2 result from the IS literature's analysis and our experience in this field, using agency theory as the basis for the development of this conceptual model (Creswell, 2009). Details about the MLR search process, including scientific and grey literature, are described in the appendix. The modeling process considered the contributions listed in Table S1, explicitly focusing on data sovereignty in the IS domain. We use examples to explain how we derived the conceptual model when explaining each core aspect. Table 2 summarizes all core aspects and relations and lists their specifications.

With directed arrows, the conceptual model illustrated in Fig. 1 represents the relations of the core conceptual aspects. The model acknowledges the data asset as its central component that must be protected in an organizational or personal context if shared with other parties (Nagel & Lycklama, 2021). During its lifecycle, from creation to sharing and deletion (Rahul & Banyal, 2020), a data asset can reach different statuses and versions because it is *modified* by activities in the data value chain (Curry, 2016). These activities are *performed* by the data provider or the data consumer who gained access to the data asset (Otto et al., 2022). In order to implement data sovereignty, the provider and consumer must *negotiate* a contract that *specifies the use conditions of* the data asset (Zrenner et al., 2019). Access and usage policies are possible examples of such contracts (Gil et al., 2020). Due to frequent mistrust between the parties involved (Lauf et al., 2021), a data provider often seeks to ensure that the consumer only performs data value chain activities described in the contractual agreement. Therefore, a manual or technical data infrastructure helps *ensure* trust because it *supports the management of* contracts through enforcement techniques (Munoz-Arcentales et al., 2019). Nevertheless, trust is always *required* by all stakeholders involved (Nagel & Lycklama, 2021), even if the concept reduces the minimum amount needed to create a data sovereignty solution. The following subsections describe every core aspect in detail.

Data asset

Based on the conceptual model, data sovereignty can be defined as an instrument to keep control over an actor's data asset. Examples of data assets can range from individual files to complete batches and full data streams. Such *data assets* must be controlled in terms of their access and usage (Munoz-Arcentales et al., 2019). Data are defined as assets describing intangible objects that can be reproduced repeatedly (Capiello et al., 2020). However, it is worth noting that there is no single definition of the concept in IS research (McKinney & Yoos, 2010). Data are contextual, and their ownership is difficult to define. They cannot be classified as private or common goods, such as traditional commodities (Jentzsch, 2018), since there are no legally binding concepts regarding their ownership (Bärenfänger, 2017). The data asset has been placed at the base of the model as it is key for each application of data sovereignty. Since the status of the data asset is modified by the data value chain and lifecycle activities, they are directly related to the data asset and positioned at the bottom as a baseline.

Data provider and data consumer

A *data provider* can decide to keep their data private for internal use, share it publicly, or allow access to a restricted number of third parties based on custom rules. For example,

contracts are created and negotiated between the data provider and the *data consumer* to keep control over the data asset. Providers and consumers can be individuals, enterprises, or organizations sharing data assets (Cavanillas et al., 2016; Marfia et al., 2017). In the case of a contractual agreement, the provider can be further divided into the role of a *data owner* that creates and executes control over the data asset and authorizes a data provider to make it available to other parties (Hummel et al., 2021; Otto et al., 2019). In addition, when referring to data consumer, other sources, such as the Data Spaces Support Centre Glossary, use the term *data recipient* (Data Spaces Support Centre, 2023a). Besides contractual arrangements between both partners, data-providing enterprises can share data directly or through existing systems, such as data marketplaces (Nagel & Lycklama, 2021). Here, a data consumer can buy either the data asset itself or limited usage rights. Since both actors are represented as core aspects in the model, they are placed on the left side for the provider part and on the right for the consumer part, as all activities are performed in between them.

Contractual agreement

As stated above, exercising data sovereignty can promote data sharing between organizations. In the traditional sense, written contracts are drawn up to increase trust, which results in a contractual agreement after mutual consent. Due to a lack of control, these agreements are often not fully honored and lack high levels of trustworthiness (Nagel & Lycklama, 2021). IS research has recognized and addressed this problem to enforce *contract agreements* that are negotiated and monitored semi-automatedly with the help of infrastructures and architectures to reduce (un)intentional data misuse (Jarke et al., 2019). Therefore, different systems and processes in various domains focus on smart contracts (Ghazizadeh & Sun, 2021). The data provider and consumer can be two neutral actors creating a contract based on rights and obligations, data usage policies, and terms and conditions (Zrenner et al., 2019), described in more detail in the infrastructure section. They can give or revoke their consent to change access rights and specify conditions of how their data can be accessed and used. The contractual agreement is located in the middle, as it consists of the main conditions for maintaining control over data assets — the main goal of data sovereignty.

Data value chain and data lifecycle activities

As depicted in Fig. 1, the *data value chain* includes different activities in the *data lifecycle* of a data asset: creation, storage, usage, sharing, archiving, and destruction (Rahul & Banyal, 2020). In this context, the implementation of data sovereignty enables an organization or individual to control the data asset throughout the data lifecycle. According to Curry (2016), an information flow consists of different activities that perform transformation steps to turn a data input into a data output. In the context of data sovereignty, the ability to keep control must extend over all data value chain activities, from creation to transformation to deletion, rather than focusing on individual activities (Banse, 2021). The activities must be consistent with the contractual agreements and usage conditions to enable self-determination. Accordingly, the data asset itself in Fig. 1 is not directly linked to the data provider or consumer (Nagel & Lycklama, 2021). Instead, the data provider and data consumer perform value chain activities on the data asset.

Data infrastructure

The data infrastructure component enforces terms and conditions determined in the contractual agreement (Munoz-Arcentales et al., 2019; Nagel & Lycklama, 2021). It is centrally located in the model since it works between the data provider and consumer by validating and executing terms and restrictions (Nagel & Lycklama, 2021), specified in the contractual agreement (see Fig. 1). These terms are divided into access control (AC) and usage control (UC), which protect data assets in almost all activities in the data value chain and lifecycle. As implied by the term AC, the concept focuses on the concrete control of access. Seeing as control is lost once access is granted, UC extends the control over data before and after third-party access (Gil et al., 2020), specifying which aspects of actors in ecosystems can access and use the data (Zrenner et al., 2019). However, AC and UC requirements specified in contractual agreements do not add value if not enforced correctly. Therefore, data infrastructure components, such as software systems, must validate the conditions of the contractual agreement and execute the actions described in the policies (Gil et al., 2020). Concepts based on decentralized identities (Ernstberger et al., 2023) and initiatives, such as the International Data Spaces Association (IDSA) and GAIA-X, operate according to standards and the technical implementation of data infrastructure components to address these problems. Their solutions find application in various domains, such as the cloud, IoT devices (Qarawlus et al., 2021), manufacturing (Landolfi et al., 2019), and many others.

Trust

According to Schilke and Cook (2013), trust has emerged as a central theme in inherently uncertain relationships, with Botsman (2017) defining the term as the "confident relationship with the unknown" (2017, p. 8). While in private and closed scenarios, trust can be established in the first instance because the actors know each other, it is challenging in the

second scenario as the data provider and consumer are partly unknown due to complex supply chain networks with many participants (Gil et al., 2020). In the conceptual model, the relationship of trust needs to be considered from two different angles. In the first step, trust is required by the data provider and consumer (Peterson et al., 2011). In this context, actors in open and closed data ecosystems must establish a fundamental trust relationship in the methods and technologies used to enter a relationship and realize data sovereignty. In the second step, trust can be enhanced as soon as parties, such as data providers and consumers, establish contractual agreements via data-sharing infrastructure to accelerate business transactions (Yang et al., 2021). Thus, the basic trust required by data consumers and providers helps strengthen the overall trust in the data infrastructure that enforces the policies specified in the contract agreements. To make the argument of trust a core aspect for developing a more robust conceptual model, Munoz-Arcentales et al. (2019) stated: "*Trust.* It is the basis for all the relations between different organizations. Thus, being part of trusted environments is a key part of every operation, including data exchange. Data usage control is achieved thanks to this principle" (2019, p. 592), which makes it an essential component of data sovereignty.

Examples from the field

The model was evaluated by concrete examples from the field. Such real-life scenarios can demonstrate its usefulness and possible applications. One example stems from the German automotive industry and deals with data exchange in the supply chain. The case study, its requirements, and the results presented by Opriel et al. (2021) can be mapped to the core aspects. In their study, the data exchange occurs between an original equipment manufacturer (OEM) and a specific supplier (data provider, data consumer). They exchange industrial information on demand and capacity (data assets) at different stages (data value chain and lifecycle activities) based on such current standards as the Electronic Data Interchange (EDI) (data infrastructure). The researchers identified the need for trust and the possibilities of contractual agreements in their problem, barriers, and business requirements analysis: "[Data sovereignty] can foster trust in each other and reduce risks being affected in data breaches (P16) […]. In order to secure legal aspects, the system shall provide functionalities to link usage policies with contractual definitions (R16)" (Opriel et al., 2021, p. 436). Here, the instrument of data sovereignty is implemented to overcome trust issues originating from power imbalances between participating actors and, therefore, serves as an excellent example of agency theory's applicability.

Another concrete example explains the shared use of data in a network of enterprises. In its white paper, Plattform Industrie 4.0 (2022) demonstrated how the technical implementation of data sovereignty plays a crucial role in multilateral data sharing for Collaborative Condition Monitoring (CCM) between such participants as component suppliers and factory operators (data provider, data consumer). They share and use (data value chain and lifecycle activities) datasets, such as sensor data (data asset), to leverage data-driven business models via a decentralized, federated infrastructure (Plattform Industrie 4.0, 2022). Similar to the previous case, the core aspects of the conceptual model can be directly mapped to their results, as summarized in Table 3. Component suppliers, machine suppliers, and factory operators create legally binding concepts to ensure trust between each other. Moreover, this example showcases agency theory's relevance in this actor relationship and highlights that data sovereignty is a suitable instrument with which to overcome mistrust and weaken power imbalances, even if both actors have their own interests.

Discussion and future research opportunities

The presented conceptual model offers a new approach to understanding data sovereignty's implementation in IS research by considering adjacent domains. It contributes to the existing literature by laying the foundation for further research, as well as by filling the above-described research gaps of underlying conflicts and inconsistencies. The following discussion describes the study's practical and theoretical implications and addresses current limitations and future research opportunities.

This study's results lead to direct implications for practice, as they serve to guide and provide a mutual understanding of the concept for individuals and companies. It aims to help users technically implement data sovereignty, e.g., actors in research projects, organizations building data-sharing ecosystems, and stakeholders strengthening the role of data sovereignty through regulatory bodies. In addition, industry and research projects related to IDSA or Gaia-X can help to further communicate and develop this topic by designing systems based on data sovereignty principles. Additionally, individuals and society can play an enhanced role in demanding technology that implements data sovereignty for all data lifecycle stages by design, in line with European values. The conceptual model can further refine this vision and clarify communication.

For theory, this work's conceptual model can be seen as a necessary academic addition to ongoing discussions. The terminological ambiguity, viewpoints of current research streams, and existing definitions were brought together by defining and describing core aspects. We acknowledge that, in IS research, other models have sought to offer a mutual understanding of

Table 3 Examples mapped to the core conceptual data sovereignty aspects

Core aspects	Example 1: Demand and Capacity Management in the Automotive Supply Chain (Opriel et al., 2021)	Example 2: Collaborative Condition Monitoring of Industrial Assets (Plattform Industrie 4.0, 2022)
Data asset	Industrial information for demand and capacity	Datasets, such as sensor data
Data provider and data consumer	OEM (car manufacturer) and their Tier 1 supplier	Component supplier, machine supplier, and factory operator
Contract agreement	Currently used paper-based contracts should be replaced by usage policies linked to contract definitions.	Currently used bilateral contracts should be replaced by data licenses to specify usage restrictions.
Data value chain and data lifecycle activities	All lifecycle activities (from creation to sharing to deletion) with a focus on data exchange.	Data usage/data sharing
Infrastructure	Currently used manual data exchange and EDI standards should be extended by decentralized platforms.	Use of federated infrastructures on a cross-industry basis based on the Asset Administration Shell (IDTA, 2023)
Trust	Since trust is identified as a major attribute, it can be strengthened by the implementation of usage control.	Data space providers and operators must create legally binding concepts to ensure trust between participants.

data sovereignty. However, Ernstberger et al.'s (2023) model has a nearly exclusive technical layer perspective, while Zrenner et al.'s (2019) applies it in the manufacturing domain only, and the model of Otto et al. (2019) is a specific reference architecture. An additional theoretical impact arises from linking different research streams that describe the core conceptual aspects. To the best of our knowledge, some of these (e.g., the data value chain and trust) had not previously been contextualized in this manner, meaning that this study offers an approach with the potential to open up new perspectives. Due to its fundamentality, this IS research's theoretical contributions can be tested and applied in different research areas, e.g., with a legal or political focus.

Despite careful evaluation, this fundamentals study suffers from limitations as it could not cover all essential research strands. Nevertheless, these can provide input for future research opportunities according to different paradigms, namely design science research (DSR), which aims to develop artifacts addressing real-world problems (Hevner et al., 2004), and behavioral research focusing on why groups or individuals act in a specific way and how they can be influenced (Skinner, 1965). To theoretically ground the conceptual model, the agency theory approach was chosen. However, its limitation must be acknowledged, which include, for example, a closer relation to the area of IS, defined "as a system[s] in […] organization[s]" (Davis, 2000, p. 67). Moreover, the literature analyses have limitations since using different databases or searches could lead to different results.

In line with the DSR paradigm, further limitations are addressed in Table 4 and described in the following: First, future research should examine the necessary development of an artifact that supports individuals in controlling their data (*RQ#1*). Moreover, the implementation of data sovereignty according to the model for individuals is valid; nevertheless, its enforcement requires further attention. Research on the enforcement of data sovereignty for individuals exists (Lomotey et al., 2022). However, as this was outside the scope of this study, future research could explore which artifacts need to be developed to enhance individuals' ability to control their data. Additionally, the future development of the instrument of data sovereignty was not covered in this research. Therefore, identifying the capabilities needed to implement data sovereignty as an instrument is critical (*RQ#2*). Building on this, conducting design-oriented studies of maturity models to track and measure data sovereignty's implementation (*RQ#3*) could be a promising research direction. Furthermore, there is a need for IT artifacts in policy management and data spaces, as well as reference models and methods, to establish, develop, improve, and ensure data sovereignty in internal and external data management activities *(RQ#4)*, such as validation, enforcement, signing, watermarking, or data integrity concepts (Hellmeier et al., 2023).

In the context of this study's limitations, the behavioral research paradigm applies to various research opportunities. Due to this research's qualitative literature approach, subjectivity can be seen as a limitation. Even if examples from the field are mapped to the conceptual model (Opriel et al., 2021; Plattform Industrie 4.0, 2022), applying the model in practice, e.g., in the "common European data spaces" (Data Spaces Support Centre, 2023b, p. 5) would prove its utility in various data sharing projects (*RQ#5*). Additionally, this could help validate agency theory's application for reaching an overall understanding of implementing data sovereignty as an instrument. Moreover, the cost of such implementation has not been discussed in this research. The relationship between the value of data and data economics on the one hand, and data sovereignty on the other, acknowledging that data assets may vary in criticality and value, is an exciting research strand. Open questions have to be answered focusing on the maintenance costs of data infrastructure and standards for enforcement (*RQ#6*). Besides, data sovereignty is a prerequisite for enabling more data sharing (Azkan et al., 2022). This study has not explicitly analyzed whether data

Table 4 Summary of future research opportunities

Design science research		
Example	Research question	
Enforcing data sovereignty for individuals	What artifacts need to be developed to enhance individuals' ability to control their data?	*RQ#1*
Capabilities of data sovereignty	What is the design of a model for capabilities needed to implement data sovereignty?	*RQ#2*
Maturity model for data sovereignty	What is the design of a maturity model that measures data sovereignty?	*RQ#3*
Operationalization of data sovereignty	What artifacts need to be developed to support the operationalization of data sovereignty?	*RQ#4*
Behavioral research		
Example	Research question	
Application of the conceptual model to additional practical cases in data spaces	How do data spaces apply this conceptual model?	*RQ#5*
Relationship between the value of data and data economics on the one hand, and data sovereignty on the other	Who builds, maintains, and pays for the data infrastructure? Who sets the standards and enforces the rules?	*RQ#6*
More data sharing as an incentive for the implementation of data sovereignty	How does the implementation of data sovereignty affect data sharing?	*RQ#7*

sovereignty positively or negatively impacts data sharing, thus making it necessary to explore this aspect in the future and re-evaluate the topic's importance *(RQ#7)*.

Summary

As IS research on data sovereignty remains in its infancy, this study has included academic and practical literature in its investigation so as to determine a common understanding of the concept itself (see Fig. 1). As shown by the analysis of the current research stream, data sovereignty is not uniformly defined, with contrasting explanations and definitions having been offered. This fundamentals paper expands IS research's knowledge on data sovereignty by providing a conceptual model following agency theory and validated by documented real-world examples. It emphasizes the specification of the core aspects (derived from the literature) needed to implement data sovereignty. The technological implementation of data sovereignty is essential for guaranteeing trusted data sharing between individuals and organizations of different parties and make innovation happen. However, further practical and theoretical implications have yet to be uncovered, and future research must still evaluate and apply the proposed model.

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1007/s12525-024-00693-4.

Funding Open Access funding enabled and organized by Projekt DEAL.

References

Azkan, C., Gür, I., Hupperz, M., Gelhaar, J., Gieß, A., Groß, T., Frings, S., Kett, H., Kutzias, D., Strauß, O., Büchel, J., Demary, V., Engels, B., Goecke, H., Mertens, A., Röhl, K.-H., Rusche, C., Scheufen, M., Schröder, B., & Valet, S. (2022). *Incentives and economics of data sharing: Fields of action of cross-company data exchange and status quo of the German economy*. https://ieds-projekt.de/wp-content/uploads/2022/08/IEDS-Whitepaper_Englisch.pdf. Accessed 12 Dec 2023

Banse, C. (2021). Data sovereignty in the cloud - Wishful thinking or reality? *Conference on Computer and Communications Security*, 153–154. https://doi.org/10.1145/3474123.3486792

Bärenfänger, R. (2017). *Managing information services in the digital economy*. Difo-Druck GmBh.

Botsman, R. (2017). *Who can you trust? How technology brought us together and why it might drive us apart* (First edition). Public Affairs.

Capiello, C., Gal, A., Jarke, M., & Rehof, J. (2020). *Data ecosystems: Sovereign data exchange among organizations* (Dagstuhl Seminar 19391), pp. 66–134. https://doi.org/10.4230/DagRep.9.9.66

Cavanillas, J. M., Curry, E., & Wahlster, W. (2016). *New horizons for a data-driven economy*. Springer International Publishing. https://doi.org/10.1007/978-3-319-21569-3

Chander, A., Abraham, M., Chandy, S., Fang, Y., Park, D., & Yu, I. (2021). Achieving privacy. *SMU Law Review, 74*(4), 607–664.

Chapin, F. S., Matson, P. A., & Vitousek, P. M. (2011). *Principles of terrestrial ecosystem ecology*. Springer, New York. https://doi.org/10.1007/978-1-4419-9504-9

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). Sage.

Curry, E. (2016). *The big data* value *chain: Definitions, concepts, and theoretical approaches*. https://doi.org/10.1007/978-3-319-21569-3_3

Data Spaces Support Centre. (2023a). *Blueprint Version 0.5* (No. 1.0). https://dssc.eu/space/BPE/179175433/Data+Spaces+Blueprint+%7C+Version+0.5+%7C+September+2023. Accessed 12 Dec 2023

Data Spaces Support Centre. (2023b). *Starter kit for data space designers* (No. 1.0). https://dssc.eu/space/SK/29523973/Starter+Kit+for+Data+Space+Designers+%7C+Version+1.0+%7C+March+2023. Accessed 12 Dec 2023

Davis, G. B. (2000). Information systems conceptual foundations: Looking backward and forward. In R. Baskerville, J. Stage, & J. I. DeGross (Eds.), *IFIP advances in information and communication technology. Organizational and social perspectives on information technology* (Vol. 41, pp. 61–82). US: Springer.

Docter, Q., & Fuchs, C. (Eds.). (2020). *CompTIA cloud essentials+ study guide*. Wiley. https://doi.org/10.1002/9781119642138

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *The Academy of Management Review, 14*(1), 57. https://doi.org/10.2307/258191

Ernstberger, J., Lauinger, J., Elsheimy, F., Zhou, L., Steinhorst, S., Canetti, R., Miller, A., Gervais, A., & Song, D. (2023). SoK: Data sovereignty. *2023 IEEE 8th European Symposium on Security and Privacy (EuroS&P)* (pp. 122–143). IEEE. https://doi.org/10.1109/EuroSP57164.2023.00017

Esposito, C., Castiglione, A., & Choo, K.-K.R. (2016). Encryption-based solution for data sovereignty in federated clouds. *IEEE Cloud Computing, 3*(1), 12–17. https://doi.org/10.1109/MCC.2016.18

European Commission. (2020). *Proposal for a Regulation of the European Parliament and of the Council on European Data Governance (Data Governance Act)* (COM/2020/767 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0767. Accessed 12 Dec 2023

European Commission. (2022). *Proposal for a regulation of the european parliament and of the council on harmonised rules on fair access to and use of data (Data Act)* (COM/2022/68 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0068. Accessed 12 Dec 2023

Garousi, V., Felderer, M., & Mäntylä, M. V. (2019). Guidelines for including grey literature and conducting multivocal literature reviews in software engineering. *Information and Software Technology, 106*, 101–121. https://doi.org/10.1016/j.infsof.2018.09.006

Gelhaar, J., Groß, T., & Otto, B. (2021). A taxonomy for data ecosystems. *Proceedings of the 54th Hawaii International Conference on System Sciences*, 6113–6122. https://doi.org/10.24251/HICSS.2021.739

German Ethics Council. (2017). *Big Data and Health – Data Sovereignty as the Shaping of Informational Freedom: Executive Summary & Recommendations*. 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. Accessed 12 Dec 2023

Ghazizadeh, E., & Sun, T. (2021). A systematic literature review of smart contract applications. In K. Arai, S. Kapoor, & R. Bhatia (Eds.), *Advances in intelligent systems and computing: Vol. 1290. Proceedings of the Future Technologies Conference (FTC) 2020, Volume 3* (Vol. 1290, pp. 877–888). Springer International Publishing. https://doi.org/10.1007/978-3-030-63092-8_59

Gil, G., Arnaiz, A., Diez, F. J., & Higuero, M. V. (2020). Evaluation methodology for distributed data usage control solutions. *2020 Global Internet of Things Summit (GIoTS)* (pp. 1–6). IEEE. https://doi.org/10.1109/GIOTS49054.2020.9119565

Grant, P. (1983). Technological sovereignty: Forgotten factor in the "Hi-Tech" Razzamatazz. *Prometheus, 1*(2), 239–270. https://doi.org/10.1080/08109028308628930

Hellmeier, M., Pampus, J., Qarawlus, H., & Howar, F. (2023). Implementing data sovereignty: Requirements & challenges from practice. *Proceedings of the 18th International Conference on Availability,* Reliability *and Security* (pp. 1–9). ACM. https://doi.org/10.1145/3600160.3604995

Hellmeier, M., & von Scherenberg, F. (2023). A delimitation of data sovereignty from digital and technological sovereignty. *ECIS 2023 Research Papers*. https://aisel.aisnet.org/ecis2023_rp/306. Accessed 12 Dec 2023

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75–105. https://doi.org/10.2307/25148625

Hinsley, F. H. (1986). *Sovereignty* (2. ed.). Cambridge University Press.

Hojati, M., Farmer, C., Feick, R., & Robertson, C. (2021). Decentralized geoprivacy: Leveraging social trust on the distributed web. *International Journal of Geographical Information Science, 35*(12), 2540–2566. https://doi.org/10.1080/13658816.2021.1931236

Hong, S., & Kim, H. (2020). VaultPoint: A blockchain-based SSI model that complies with OAuth 2.0. *Electronics, 9*(8), 1231. https://doi.org/10.3390/electronics9081231

Houy, C., Fettke, P., & Loos, P. (2012). Understanding understandability of conceptual models – What are we actually talking about? In D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, M. Naor, O. Nierstrasz, C. Pandu Rangan, B. Steffen, M. Sudan, D. Terzopoulos, D. Tygar, M. Y. Vardi, G. Weikum, P. Atzeni, D. Cheung, & S. Ram (Eds.), *Lecture Notes in Computer Science. Conceptual Modeling* (Vol. 7532, pp. 64–77). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-34002-4_5

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society, 8*(1). https://doi.org/10.1177/2053951720982012

IDTA. (2023). *Specification of the asset administration shell - Part 1: Metamodel.* Industrial Digital Twin Association. https://industrialdigitaltwin.org/wp-content/uploads/2023/04/IDTA-01001-3-0_SpecificationAssetAdministrationShell_Part1_Metamodel.pdf. Accessed 12 Dec 2023

Irion, K. (2012). Government cloud computing and the policies of data sovereignty. *Policy and Internet*, *4*(3-4). https://doi.org/10.2139/ssrn.1935859

Janssen, M., Charalabidis, Y., & Zuiderwijk, A. (2012). Benefits, adoption barriers and myths of open data and open government. *Information Systems Management, 29*(4), 258–268. https://doi.org/10.1080/10580530.2012.716740

Jarke, M., Otto, B., & Ram, S. (2019). Data sovereignty and data space ecosystems. *Business & Information Systems Engineering, 61*(5), 549–550. https://doi.org/10.1007/s12599-019-00614-2

Jentzsch, N. (2018). *Dateneingentum - Eine gute Idee für die Datenökonomie?* [Data ownership - A good idea for the data economy?]. https://www.stiftung-nv.de/de/publikation/dateneigentum-eine-gute-idee-fuer-die-datenoekonomie. Accessed 12 Dec 2023

Kuhrmann, M., Fernández, D. M., & Daneva, M. (2017). On the pragmatic design of literature studies in software engineering: An

experience-based guideline. *Empirical Software Engineering, 22*(6), 2852–2891. https://doi.org/10.1007/s10664-016-9492-y

Kushwaha, N., Roguski, P., & Watson, B. W. (2020). Up in the air: Ensuring government data sovereignty in the cloud. *2020 12th International Conference on Cyber Conflict (CyCon)* (pp. 43–61). IEEE. https://doi.org/10.23919/CyCon49761.2020.9131718

Labadie, Clément., & Legner, C. (2019). Understanding data protection regulations from a data management perspective: A capability-based approach to EU-GDPR. *14th International Conference on Wirtschaftsinformatik,*, 1292–1306. https://aisel.aisnet.org/wi2019/track11/papers/3/. Accessed 12 Dec 2023

Landolfi, G., Barni, A., Izzo, G., Fontana, A., & Bettoni, A. (2019). A MaaS platform architecture supporting data sovereignty in sustainability assessment of manufacturing systems. *Procedia Manufacturing, 38*(38), 548–555. https://doi.org/10.1016/j.promfg.2020.01.069

Lauf, F., Scheider, S., Meister, S., Radic, M., Herrmann, P., Schulze, M., Nemat, A. T., Becker, S. J., Rebbert, M., Abate, C., Konrad, R., Bartsch, J., Dehling, T., & Sunyaev, A. (2021). *Data sovereignty and data economy—Two repulsive forces?* https://doi.org/10.24406/isst-n-634865

Lomotey, R. K., Kumi, S., & Deters, R. (2022). Data trusts as a service: Providing a platform for multi-party data sharing. *International Journal of Information Management Data Insights, 2*(1), 100075. https://doi.org/10.1016/j.jjimei.2022.100075

Marfia, F., Fornara, N., & Nguyen, T.-V.T. (2017). A framework for managing data provider and data consumer semantic obligations for access control. *AI Communications, 30*(1), 67–82. https://doi.org/10.3233/AIC-170725

McKinney, E. H., & Yoos, C. J. (2010). Information about information: A taxonomy of views. *MIS Quarterly, 34*(2), 329. https://doi.org/10.2307/20721430

Munoz-Arcentales, A., López-Pernas, S., Pozo, A., Alonso, Á., Salvachúa, J., & Huecas, G. (2019). An architecture for providing data usage and access control in data sharing ecosystems. *Procedia Computer Science, 160*(160), 590–597. https://doi.org/10.1016/j.procs.2019.11.042

Nagel, L., & Lycklama, D. (2021). *Design principles for data spaces* - Position paper. https://doi.org/10.5281/zenodo.5105744

Oliveira, M. I. S., & Lóscio, B. F. (2018). What is a data ecosystem? In M. Janssen, S. A. Chun, V. Weerakkody, A. Zuiderwijk, & C. C. Hinnant (Eds.) *Proceedings of the 19th Annual International Conference on Digital Government Research: Governance in the Data Age* (pp. 1–9). ACM. https://doi.org/10.1145/3209281.3209335

Opriel, S., Möller, F., Burkhardt, U., & Otto, B. (2021). Requirements for usage control based exchange of sensitive data in automotive supply chains. *Proceedings of the 54th Hawaii International Conference* on *System Sciences*, 431–440. https://doi.org/10.24251/HICSS.2021.051

Otto, B., ten Hompel, M., & Wrobel, S. (2022). Designing data spaces. *Springer International Publishing*. https://doi.org/10.1007/978-3-030-93975-5

Otto, B., Steinbuss, S., Teuscher, A., & Lohmann, S. (2019). *Ids Reference Architecture Model* (No. 3.0). https://doi.org/10.5281/ZENODO.5105529

Peterson, Z. N. J., Gondree, M., & Beverly, R. (2011). 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*. https://dl.acm.org/doi/10.5555/2170444.2170453

Plattform Industrie 4.0. (2022). *Multilateral data sharing in industry: Concept using "Collaborative Condition Monitoring" as a basis for new business models*. https://www.plattform-i40.de/IP/Redaktion/EN/Downloads/Publikation/Multilateral_Data_Sharing.pdf. Accessed 12 Dec 2023

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1532

Polatin-Reuben, D., & Wright, J. (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*. https://www.usenix.org/conference/foci14/workshop-program/presentation/polatin-reuben. Accessed 12 Dec 2023

Qarawlus, H., Hellmeier, M., Pieperbeck, J., Quensel, R., Biehs, S., & Peschke, M. (2021). Sovereign data exchange in cloud-connected IoT using international data spaces. *2021 IEEE Cloud Summit (Cloud Summit)* (pp. 13–18). IEEE. https://doi.org/10.1109/IEEECloudSummit52029.2021.00010

Rahul, K., & Banyal, R. K. (2020). Data life cycle management in big data analytics. *Procedia Computer Science, 173*, 364–371. https://doi.org/10.1016/j.procs.2020.06.042

Sarabia-Jacome, D., Lacalle, I., Palau, C. E., & Esteve, M. (2019). Enabling industrial data space architecture for seaport scenario. *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)* (pp. 101–106). IEEE. https://doi.org/10.1109/WF-IoT.2019.8767216

Schilke, O., & Cook, K. S. (2013). A cross-level process theory of trust development in interorganizational relationships. *Strategic Organization, 11*(3), 281–303. https://doi.org/10.1177/1476127012472096

Schinle, M., Erler, C., & Stork, W. (2021). Data sovereignty in data donation cycles - Requirements and enabling technologies for the data-driven development of health applications. *Proceedings of the 54th Hawaii International Conference on System Sciences*, 3972–3981. https://doi.org/10.24251/HICSS.2021.482

Singi, K., Choudhury, S. G., Kaulgud, V., Bose, R. J. C., Podder, S., & Burden, A. P. (2020). Data sovereignty governance framework. *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops* (pp. 303–306). ACM. https://doi.org/10.1145/3387940.3392212

Skinner, B. F. (1965). *Science and human behavior*. New York, NY: The Free Press.

Statista. (2022). *Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2030*. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

Tan, K.-L., Chi, C.-H., & Lam, K.-Y. (2022). *Analysis of digital sovereignty and identity: From digitization to digitalization.* https://doi.org/10.48550/arXiv.2202.10069

Taylor, J., & Kukutai, T. (Eds.). (2016). *Research monograph / Centre for Aboriginal Economic Policy Research, College of Arts and Social Sciences, The Australian National University, Canberra: no. 38. Indigenous data sovereignty: Toward an agenda*. Australian National University Press. http://www.jstor.org/stable/10.2307/j.ctt1q1crgf

van den Homberg, M., & Susha, I. (2018). Characterizing data ecosystems to support official statisticswith open mapping data for reporting on sustainable development goals. *ISPRS International Journal of Geo-Information, 7*(12), 456. https://doi.org/10.3390/ijgi7120456

Verhulst, S. G. (2023). Operationalizing digital self-determination. *Data & Policy, 5*, e14. https://doi.org/10.1017/dap.2023.11

Watson, R. T., & Webster, J. (2020). Analysing the past to prepare for the future: Writing a literature review a roadmap for release 2.0. *Journal of Decision Systems, 29*(3), 129–147. https://doi.org/10.1080/12460125.2020.1798591

Yang, R., Liu, N., Pang, Z., Wang, Y., Jia, Q., Lu, W., Li, Z., Li, M., & Wu, L. (2021). The next generation identity platform for digital era based on blockchain. *Lecturer Notes in Electrical Engineering, 677*(677), 1035–1044. https://doi.org/10.1007/978-981-33-4102-9_124

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