Aug 10th, 12:00 AM

Decentralizing Data Governance: A Case Study in TELCO Data Ecosystems

Vitor Hugo Machado Ribeiro
University of Coimbra, vhribeiro@dei.uc.pt

João Barata
University of Coimbra, barata@dei.uc.pt

Paulo Rupino da Cunha
University of Coimbra, rupino@dei.uc.pt

Decentralizing Data Governance: A Case Study in TELCO Data Ecosystems

Completed Research

Vítor Ribeiro
University of Coimbra, CISUC, DEI
Coimbra, Portugal
vhribeiro@dei.uc.pt

João Barata
University of Coimbra, CISUC, DEI
Coimbra, Portugal
barata@dei.uc.pt

Paulo Rupino da Cunha
University of Coimbra, CISUC, DEI
Coimbra, Portugal
rupino@dei.uc.pt

Abstract

Data governance is crossing organizational boundaries. However, governance mechanisms for data ecosystems have particularities, and tools to assist companies in steering decentralized data governance are lacking. This paper addresses these two gaps by presenting the results of a case study in the telecommunications industry (TELCO). After evaluating seventeen data governance maturity models and modeling the network actors' architecture, we classify data governance mechanisms across different companies according to the most prevailing profile of (1) data consumer, (2) data producer, and (3) data prosumer. Our findings confirm the significant differences in governing data ecosystems and present foundational data governance mechanisms for socio-technical networks. The results offer a starting point for the required data governance dimensions of more advanced maturity models crucial to developing a data ecosystem. For practice, our work illustrates essential decentralized data governance mechanisms in a highly regulated sector of the economy.

Keywords

Case study, data ecosystem, decentralized data governance, maturity model.

Introduction

Data is becoming increasingly central for business, requiring robust governance practices that specify the "*decision rights and accountabilities for an organization's decision-making about its data* (…)" (Abraham et al., 2019). On the other hand, collaborative business networks are also expanding, aiming to combine resources, create synergies, and develop capacities to quickly adapt to changes in the market and seize new opportunities. These partnerships often lead to the creation of innovative data-based products and services (Rasouli et al., 2016; Winter & Davidson, 2019). Nevertheless, with it comes a sense of loss of control over decentralized data (Lis & Otto, 2020) and difficulties defining data ownership and accountability (e.g., distributed data assets and access control).

These trends drive the need for new mechanisms capable of handling the decentralized governance of data (Jagals & Karger, 2021). According to the TM Forum (2022), one of the most critical steps is the assessment of data governance maturity. It aims at overseeing, diagnosing, assessing, and improving an organization's data governance capacities. This requires evaluating how the organization performs in various dimensions of data governance (e.g., data quality, data security, data architecture) (DAMA International, 2009) based on a set of criteria defined by the maturity model. Metadata, ownership, and other related mechanisms can facilitate traceability and interoperability in inter-organizational scenarios (Abraham et al., 2019). However, existing data governance approaches and maturity models are primarily

geared toward a single company, lacking "*methods for effective Data Ecosystems governance and control*" (Marcelo et al., 2019). Therefore, the following research question is identified:

RQ: *What are the necessary mechanisms for implementing decentralized data governance in data ecosystems that should be reflected in data governance maturity dimensions?*

We conducted a comprehensive literature review to identify seventeen data governance maturity models produced by academia and industry. Next, we performed a case study with a global multinational TELCO group. This group holds companies operating in different geographical locations subject to distinct regulations, separate power structures, and at different stages of data governance maturity.

The remainder of this paper is structured as follows. The basic concepts of decentralized data governance in data ecosystems and data governance maturity models are described. Subsequently, the research methodology is presented. Afterward, a set of dimensions for data governance maturity models are proposed and described. The case study findings are then detailed, and the paper closes with the conclusions, the limitations, and future work opportunities.

Background

Decentralized Data Governance in Data Ecosystems

Data ecosystems can be defined as complex socio-technical networks that enable collaboration between organizations in order to explore data assets (Marcelo et al., 2019). Such networks provide an environment to create and manage data sharing initiatives. Due to the fast changes in markets, technologies, new regulations, and events, organizations must be prepared to face the need to update and adapt their data governance continuously, establishing a cross-organizational data agenda, defining methods to seize market opportunities, managing data-related risks, adhering to legislation, and improving data quality (Abraham et al., 2019). Therefore, collaborative partnerships require the development and implementation of new governance mechanisms (Jagals & Karger, 2021).

Organizations can be placed into three main categories according to their strategy to use data: (1) data consumers, (2) data producers, or (3) data prosumers (Jussen et al., 2023). On the one hand, data is considered a means to develop or improve existing solutions by data consumers (Marcelo et al., 2019). Data producers, on the other hand, generate data valuable for them and, eventually, for third-party organizations. More recently, the concept of data prosumer (data producer + data consumer) emerged, since entities are now also producing data (Zhang et al., 2018) and using it for internal consumption.

Organizations integrating partnerships need to deal with the increasing data volumes from different sources (Abraham et al., 2019) and the uncertainty regarding the accountability of data and operations, the tensions in the hierarchy and power of each organization, and the use and management of data for each involved organization (Lis & Otto, 2021). Therefore, inter-organizational collaboration on the sharing and use of data becomes critical to avoid the creation of silos and fully exploit new opportunities allowed by data (Nielsen et al., 2019). A structure can be created that allows participants to influence, monitor, and engage the partnership decisions and balance the needs and outcomes of the participants (Chen et al., 2021). By promoting effective decentralized governance, it is possible to align the incentives, ensure the coordination of the actions, mitigate conflicts, and create a shared vision.

The existing data governance frameworks are unsuitable for the decentralized data governance context (Jagals & Karger, 2021). Decentralized data governance requires mechanisms to monitor data usage, define data ownership, determine data accessibility, estimate user contribution, and identify data provenance (De Prieelle et al., 2020). Moreover, governance in data ecosystems encompasses the distribution of duties and responsibilities among the partners, the incentive mechanisms, and the level of control each partner has over the network. Maturity models are an interesting solution to assess and improve governance in data ecosystems (Marcelo et al., 2019), as presented in the next section.

Data Governance Maturity Models

Maturity models assess organizational performance in a given topic and offer improvement guidelines (de Bruin et al., 2005). The concept of the maturity model has been used for decades in the field of

information systems and is usually organized in several levels or stages (e.g., 0-initial to 5-optimized). Organizations can be assessed to determine in which one they are, and an action plan can be defined to evolve to a higher stage (Al-Ruithe & Benkhelifa, 2017). Maturity models provide an overview of the company's capabilities regarding a particular domain (e.g., security, software development) or compare their status with specific benchmarks and best practices.

Data governance maturity models enable the continuous assessment of the status of a data governance program through time, with the definition of a set of metrics that facilitate the implementation of the program, guaranteeing its sustainability and stimulating organizational change (TM Forum, 2022). On the one hand, at lower levels of maturity, there are ad-hoc procedures, undefined roles and responsibilities, a lack of shared vision for the role of data, and reactive measures for data governance. On the other hand, at higher maturity levels, the organization sees data as a strategic asset, a data governance council monitors the data governance framework, and a set of roles and responsibilities concerned with data governance are defined. Moreover, a set of processes, procedures, and policies for data governance are correctly defined, documented, and implemented (TM Forum, 2022).

Our research revealed that, in the last 15 years, several data governance maturity models have been proposed. The research in academia revealed works that are more focused on developing maturity models for specific sectors and paradigms, such as the case of cloud computing (e.g., storage management, infrastructure technology management) (Al-Ruithe & Benkhelifa, 2017), data spaces (e.g., data sharing) (Curry & Tuikka, 2022), and micro-financial organizations (e.g., data quality, metadata) (Rivera et al., 2017). The grey literature has the highest number of contributions to data governance maturity models, with most of them being developed by companies (e.g., IBM (2007)).

The works found in the literature are valuable but insufficient for adoption in data ecosystems. Existing models focus on a single organization (Marcelo et al., 2019), lacking the mechanisms to assess the implementation of decentralized data governance and address its challenges. We have identified a single proposal for decentralized data governance scenarios that include technology, people, value-creation, and accountability dimensions (Curry & Tuikka, 2022). However, this model is restricted to the data space and does not incorporate mechanisms for metadata, data quality, or data privacy. Therefore, there is a need to develop new data governance maturity models for data ecosystems (Marcelo et al., 2019).

Methodology

We started our research by reviewing decentralized data governance concepts and data governance maturity models. We followed the best practices for a literature review suggested by Webster & Watson (2002). The review focused on the identification and analysis of data governance maturity models. We used the search expression "data governance" + "maturity model", leading to 29 results in Scopus and 15 in WoS. These searches did not include restrictions regarding date ranges. First, we checked the results for duplications and reduced our sample to 30 papers. Second, we analysed the remaining papers for both original and cited data governance maturity models. Based on this sample, we identified the factors that distinguish decentralized ecosystem data governance from local data governance. We concluded that new governance mechanisms are necessary to implement inter-organizational data-sharing, coordination processes, and control of decentralized resources in data ecosystems.

Next, we applied our findings in real situations. To that end, we used an interpretivist methodology that enables the development of in-depth research adequate for the complexity of the matter we are dealing with (Klein & Myers, 1999). We conducted an in-depth case study (Yin, 2009) in a TELCO group and identified three categories of roles that organizations can take in data-based collaborative networks: data producer, data consumer, and data prosumer.

The data-gathering stage resorted to three primary sources of information, namely, (1) semi-structured interviews, (2) workshops with the TELCO group's members, and (3) internal documents (e.g., presentations and reports) related to the data governance framework. The interviews were conducted between May and September 2022 and lasted between thirty minutes and one hour and a half. We used a protocol of semi-structured interviews with only a few direct questions (Myers & Newman, 2007). We have conducted a total of six interviews and two discussion workshops with companies's experts. The interview protocol consisted of four stages. First, the interviewees targeted data scientists to identify their perception of data governance mechanisms in data science and research activities. Second, project

managers of data-based projects were interviewed. This enabled the identification of data governance mechanisms deployed within the management activities, how data is integrated and deployed in projects, performance measurement of activities related to data, and the challenges of developing data-based solutions. Third, data pivots were interviewed, responsible for monitoring regulations and their impact on each organization (e.g., defining the mechanism to embrace data privacy requirements). Lastly, we interviewed the data governance leaders, that provided us with feedback on the strategic role of data, the relationship between the several companies (e.g., the dependencies, the supply chain, the resources of each one), and the common goals of the TELCO holding for the future of decentralized data governance.

The TELCO Group

The TELCO group includes the holding, various TELCO operators, and different technology providers (e.g., software, routers, and other systems used by the group and sold to third-party organizations). These companies are involved in an ecosystem of collaboration, sharing data, IT resources, and business objectives. Despite being involved in the same group, the companies have a relatively high degree of autonomy and have established several legal agreements. The holding is responsible for guiding the partnership among the organizations, defining the major rules for collaboration, the business objectives, the principal investments, and the market strategy for the collaborative network. The technology providers involved in this scenario provide multiple services and products (e.g., platform-as-a-service solutions, data analytics tools, network devices) integrated into (internal and external) TELCO operators' offer. All these companies operate in different geographical locations, subject to distinct regulations (e.g., privacy regulations, operation restrictions), market contexts, and financial constraints.

Currently, the board of the TELCO group is gathering efforts to promote a transformation of the data governance mechanisms across several operators, as well as to deploy an IT transition of several infrastructures and services. One of the main goals is to develop and implement a set of data governance mechanisms that guarantee some standardization across the group members. The first step is to conduct a data governance maturity diagnosis to understand the current pains and strengths of the organization. This can be done using a data governance maturity model. With the assessment results, it is possible to develop an action plan for each organization according to their specific needs and context. In this context of collaboration, we can consider the existence of a maturity level for each organization and a maturity level for the group. Our initial group analysis identifies distinct data governance maturity statuses for the various organizations. The group's maturity level is important to assess the companies as a whole and to define the group's strategy. Figure 1 describes the data ecosystem architecture.

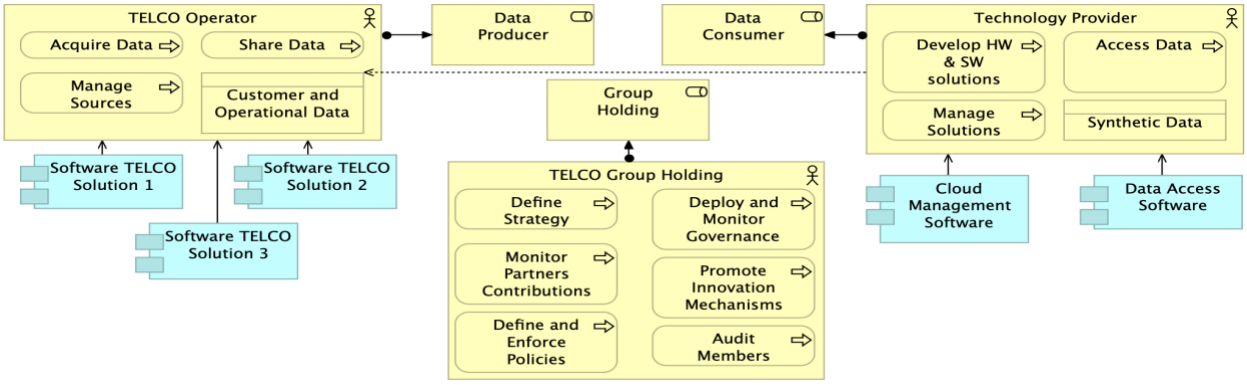

Figure 1. The ecosystem architecture of the TELCO group

Figure 1 represents the interactions between different TELCO actors using ArchiMate language (The Open Group, 2018). The elements in yellow represent the business layer (e.g., processes using the arrow notation), and the blue identify elements from the application layer. On the one hand, the technology provider companies generate and analyze internal data from their operations and synthetic data generation sources. On the other hand, they also retrieve data from the TELCO operator. TELCO operators retrieve data from the end customer's use of applications and services. Moreover, the tools used by the operator to manage the services also generate data. The TELCO operator shares the data with technology providers to improve and develop new solutions for the group.

TELCO Operator Profile

A TELCO operator provides end clients with Internet services, Pay TV, and mobile network solutions. These solutions created by the technology providers (e.g., equipment for smart homes, software for cybersecurity) allow the TELCO operator to retrieve data from the devices at the end clients' homes, providing visibility over the performance of the networks, mobile network status, and issue reporting.

The TELCO operator adheres to the profile of the data producer: it generates data from multiple sources and shares it with other group actors, according to the privacy regulations. Technology providers can use this data to develop new products, create new Artificial Intelligence (AI) and Machine Learning (ML) models, and improve existing solutions. For example, they use AI techniques to improve network performance and traffic routing. Therefore, decentralized data governance mechanisms are required. First, the organization must ensure that the data sources produce reliable data. Any inconsistencies can lead the IT experts to develop inadequate or incomplete solutions. Second, the data producer is responsible for sharing data with the other parties, requiring mechanisms to clarify and ensure ownership and responsibility over this data. Third, the TELCO operator must standardize data in a specific format agreed upon with the data consumers and prosumers to facilitate the use and sharing. Fourth, the organization must document and monitor all the data acquisition processes to show compliance with the existing regulations and the network rules for internal and external audits. Fifth, the producer must be able to identify opportunities based on the data it produces and gathers that can allow the development of new solutions by the technology providers. Lastly, the organization must guarantee the safety of the data it possesses and track and demonstrate all the changes the dataset might have had.

TELCO Technology Provider Profile

Technology providers develop customizable IT solutions for the Business-to-Business market. Therefore, it can adapt the entire development and operation lifecycle to each customer segment operating in its software-as-a-service solutions (e.g., the TELCO operator requires cloud services). For all these cases, the company can retrieve data on the operationalization of their platforms and services by the customer companies (e.g., TELCO operators). Moreover, the technology providers can also use part of the data that the end client generates to improve the TELCO products (e.g., retrieving and analyzing data from routers). Additionally, the company analyzes the data retrieved from the multiple TELCO operators of the group, providing insights for the company to develop and improve the existing solutions. Therefore, decentralized data governance mechanisms are required to guarantee accountability over data and decisions based on the data shared by the partners, data accessibility for the group members, data sharing, and compliance with regulations in distinct geographical locations (e.g., data privacy).

A scenario of a data consumer is the norm in this actor: it focuses on data analytics, developing AI and ML solutions, data integration, data visualization, and data-driven decision-making mechanisms. Moreover, the organization must manage data sources (e.g., guarantee that the sources are reliable), enable data accessibility mechanisms for the partners, acquire data from the sources, and store the data.

Towards Decentralized Data Governance Maturity Dimensions

After analyzing the seventeen data governance maturity models available in the extant literature, we identified a set of important dimensions to consider when assessing the data governance maturity of an organization, such as data architecture, data governance organization, data strategy, and data security. Table 1 describes the identified maturity dimensions suitable to data ecosystems and compares the mechanisms necessary to target each one in local and decentralized data governance contexts.

Dimension	Local Data Governance	Decentralized Data Governance
Audit Information & Logging	The organization should define a set of processes and structures for monitoring and measuring the data value, risks, and efficacy of governance (IBM, 2007).	Traceability of data governance metrics, resources, and activities (Abraham et al., 2019). Stakeholder contribution to the network assessment (Lee et al., 2017). Compliance with the network rules (Lee et al., 2017).

Dimension	**Local Data Governance**	**Decentralized Data Governance**
Data Architecture	Development and maintenance of an overall data architecture of the organization, including mechanisms for data integration, access, delivery, availability, distribution, and control (DAMA International, 2009).	Promote a standardized and trustworthy data exchange environment (Rasouli et al., 2016). Implement data integration mechanisms to manage decentralized data sources (Bruhn, 2014).
Data Governance Organization	The existence of data governance structures that conduct the implementation and monitoring of governance, communication, training of staff, leadership support, and organizational culture (Merkus et al., 2021).	New governance collaboration roles (Panian, 2010). New inter-organizational coordination units to manage decentralized dependencies and activities (Jagals & Karger, 2021). New roles to manage the contributions of each member to the partnership (Lee et al., 2017).
Data Lifecycle	The organization should define mechanisms to optimize data management throughout its lifecycle, making it efficient and contributing to its needs (Rivera et al., 2017).	Definition of data exchange standards (Rasouli et al., 2016). New processes to foster collaboration between the organizations (Panian, 2010). Ensure the interoperability of decentralized systems (Lis & Otto, 2020).
Data Policies	Data policies are the general guidelines for using data on the organization, which are influenced by the regulatory framework, standards, and strategies under which data is governed (Rivera et al., 2017). They must be defined, implemented, and enforced within the organization (TM Forum, 2022).	New data usage policies are necessary for decentralized environments (Bruhn, 2014). The data policy mechanisms must be extended to the several members of the partnership (TM Forum, 2022). Need to trace the data policies across the partners (TM Forum, 2022).
Data Risk & Compliance	This dimension covers the methodology and structures for risk management. For compliance, the organization should have defined mechanisms to track and enforce compliance with laws, policies, standards, and procedures (IBM, 2007).	Organizations must define new roles responsible for monitoring compliance that may affect the partners in different locations (Abraham et al., 2019). Identify and monitor all the legal requirements that can affect the use and sharing of different data types according to the partner's location (Lee et al., 2017).
Data Privacy	It covers the mechanisms that contribute to mitigating data leak situations, control of data access and use, and data retention (Abraham et al., 2019).	New data sharing mechanisms ensure the privacy of data (Winter & Davidson, 2019).
Data Security	The organization's mechanisms, structures, and controls to ensure data confidentiality, integrity, availability, data security planning, roles and responsibilities, and access to network management (Rivera et al., 2017).	New mechanisms for organizations to retain control over their data in decentralized settings (Abraham et al., 2019). Mechanisms are required to guarantee secure decentralized data access and sharing (Rasouli et al., 2016).
Data Stewardship and Ownership	This dimension targets mechanisms that define the accountability for the description, utilization, and standard of quality of data assets (DAMA International, 2009).	New mechanisms to define the accessibility of the distinct partners to data, clarifying who owns and accesses data (Lee et al., 2017). Decentralized data ownership must be responsible, accountable, consulted, accessible, and informed (Lee et al., 2017).

Dimension	Local Data Governance	Decentralized Data Governance
Data Strategy	The organization should define a data strategy that includes the identification of their strategic business goals, a vision statement towards the importance of the data for the organization, a set of guiding principles, a business case, long-term and short-term objectives, and an implementation roadmap for data governance (Merkus et al., 2021).	New processes and roles are required to balance organizational interests (Abraham et al., 2019). New use cases are required to define how to share or sell data without losing control (Lee et al., 2017).
Metadata	Mechanisms for describing data and IT resources by linking business and technical information, facilitating a consistent understanding of its properties and usage (TM Forum, 2022).	New metadata mechanisms to facilitate interoperability between organizations and traceability of data provenance (Abraham et al., 2019). Standardization of metadata in the partnership (Khatri & Brown, 2010)

Table 1. Data Governance Dimensions for Local and Decentralized Scenarios

Table 1 clarifies the significant differences in governing data in a local or decentralized context. These dimensions were identified by collecting, matching, and comparing the sample of data governance maturity models. We selected the dimensions that were common in at least 80% of the models. As an example, for the data lifecycle, the actors must define and enforce practical data exchange standards (Rasouli et al., 2016), develop and implement new processes that foster collaboration between them (Panian, 2010), and guarantee the interoperability of inter-organizational systems (Lis & Otto, 2020). Moreover, the traceability of data is more challenging (Abraham et al., 2019), and the standardization of metadata for the members of the collaborative network becomes a priority.

Case Study Findings

Table 2 contains the analysis of the results of our inquiries in the TELCO group, introducing the identified data governance mechanisms according to the prevalent profile of each actor. The TELCO operator acts as a data producer in the ecosystem using the Technology's Provider solutions. This data is shared with the Technology Provider, that uses this data to develop and improve solutions. The TELCO Group acts as data prosumer that produces and consumes data from external and internal sources.

Dimension	Operator (Data Producer)	Technology Provider (Data Consumer)	Network Mechanisms TELCO Group (Data Prosumer)
Audit Information & Logging	• Document data sources. • Provide the consumer with the data-acquiring process. • Define metrics to track the quality, inconsistencies, and compliance with the data-capturing process.	• Display information on how the data is used to create products and services.	• Display information on how the data is used to develop solutions. • The organizations must disclose information on the network's compliance with regulations, policies, and processes.
Data Architecture	• Handle data storage from multiple sources. • Manage sources of data, control their quality, and correct inconsistencies.	• Define mechanisms to transmit acquired data from the producer. • Define procedures to store acquired data.	• Promote a standardized and trustworthy data exchange environment. • Develop data integration mechanisms to manage decentralized data sources.

Dimension	Operator (Data Producer)	Technology Provider (Data Consumer)	Network Mechanisms TELCO Group (Data Prosumer)
Data Lifecycle	• Prepare the data according to the producer's standards and its interoperability with processes and systems.	• Document all the operations performed on data during the lifecycle.	• Define the group's data exchange standards. • Promote the interoperability of decentralized processes, resources, and systems.
Data Privacy	• Guarantee that the retrieved data does not affect citizens' privacy.	• Ensure that data-based solutions do not harm the privacy of citizens.	• Data-sharing mechanisms must ensure the privacy of data. • The solutions developed by the group and all the procedures during the lifecycle must respect the citizen's privacy.
Data Policies	• Define policies for data acquisition, security, and quality. • Ethical policies ensure respect for the citizen's privacy.	• Data policies must be targeted for using data as a product to develop new solutions. • Ethical policies ensure respect for the citizen's privacy.	• Collaboration policies promote the interaction between the partners. • Data policy roles are necessary to implement and monitor compliance with policies.
Data Security	• Promote the acquired data's integrity, security, and confidentiality.	• Define mechanisms to safely transmit, store, and dispose data.	• Define secure data sharing mechanisms.
Data Strategy	• Acquire data that is valuable for consumers to develop new data-based solutions.	• Develop new data-based solutions and improve the existing ones.	• Guarantee the autonomy of organizations to implement their strategies. • Develop a joint data strategy.
Data Stewardship and Ownership	• Document all the changes in the produced data. • Be accountable for the ownership of data provided to customers. • Ensure data accessibility to consumers.	• All the changes in the acquired data must be documented – the data consumer becomes the owner of this manipulated data.	• Ensure the accessibility of distinct partners to data. • Mechanisms define the data ownership and accountability of assets at all stages.

Table 2. Data Governance for Data Producer, Data Consumer, and Data Prosumer

Table 2 summarizes the findings of our case study for the three profiles that integrate the data ecosystem. Our analysis focused on eight of the eleven identified dimensions considering the priorities stated by the participating organizations at this stage. The decentralized data governance mechanisms are necessary for the operations and events that involve the participation of more than one organization simultaneously. This happens when organizations need to trade data and resources (e.g., the need to guarantee the safe transmission of information and avoid data leaks), the definition of the strategy of the organizations, and the decisions of the organizations that may influence or affect the remaining ones. Moreover, there is a need to define the accountability of the data providers over the shared data, create data ownership models, and monitor decentralized operations. This way, it is possible to track the changes that affect the data assets across the ecosystem and to limit data usage according to the partner's requirements.

Data producers must focus on the governance mechanisms involved in the production and acquisition of data. They need to manage their data sources by verifying and correcting the existing data inconsistencies and matching the needs and quality requirements of the customers who acquire data from them. Moreover, governance mechanisms are necessary to ensure accountability over decentralized data and data provenance. Lastly, they must consider sharing data with the data consumers, ensuring that it is according to the quality standards and requirements of the customer. Data consumers focus more on using the data for maximum business value realization and developing new products and services based on data. They must be aware of ethical issues when developing solutions, document all the changes in the acquired data, and display information on how the products are used and monitored. Decentralized data governance requires an increased deployment of inter-organizational mechanisms that can balance the stakeholders' interests while fostering an innovation culture by combining the resources and capacities of each partner. Moreover, there is the need to deploy mechanisms that allow the interoperability of systems and resources to reduce the operations that are necessary when sharing data.

Conclusion

This paper reports an in-depth case study to identify the decentralized data governance required for data producers, data consumers, and data prosumers working in data ecosystems. This research included a review of critical literature on decentralized data governance and data governance maturity models. Decentralized data governance mechanisms can support organizations in exploiting new business and market opportunities by defining a set of collaborative processes, resources, and structures that can capitalize on the capacities of each actor. These mechanisms are grouped in this paper according to the data governance dimension and the profile of the participating actors.

There are also limitations to be stated. First, the TELCO group that participated in our research does not represent the entire industry. Other actors can be considered to perform further case studies. Second, the dimensions suitable for creating decentralized data governance maturity models were identified based on the results of our literature review, in which we used a specific combination of keywords. The list can be expanded with more literature searches and insights from practitioners. Third, the research focused on the TELCO context considered a highly regulated environment. Other fields (e.g., manufacturing) may require distinct mechanisms for decentralized data governance. Lastly, we have not explored the distinct data governance mechanisms necessary for more loosely or closely coupled data ecosystems. Future work can explore how to handle data governance in these different scenarios.

Our work answers a call for developing maturity models in data ecosystems and provides the foundations for decentralized data governance. Future work may incorporate the dimensions and associated governance mechanisms in a new maturity model (or improve existing models), associating them with maturity levels. Moreover, creating a tool to support the self-assessment of data ecosystem actors and suggest governance practices would be interesting. We hope our work may inspire other researchers to contribute to the unique challenges of governance in data ecosystems that will shape many of the data-driven product developments in the future.

Acknowledgements

This work is funded by the project POWER (grant number POCI-01-0247-FEDER-070365), co-financed by the European Regional Development Fund (FEDER), through Portugal 2020 (PT2020), and by the Competitiveness and Internationalization Operational Programme (COMPETE 2020). It is also co-funded by the FCT - Foundation for Science and Technology, I.P./MCTES through national funds (PIDDAC), within the scope of CISUC R&D Unit - UIDB/00326/2020 or project code UIDP/00326/2020.

REFERENCES

Abraham, R., Schneider, J., & vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, *49*(January), 424–438.

Al-Ruithe, M., & Benkhelifa, E. (2017). Cloud data governance maturity model. *ACM International Conference Proceeding Series*.

Bruhn, J. (2014). Identifying useful approaches to the governance of indigenous data. *International*

Indigenous Policy Journal, *5*(2), 1–32.
Chen, Y., Pereira, I., & Patel, P. C. (2021). Decentralized Governance of Digital Platforms. *Journal of Management*, *47*(5), 1305–1337.
Curry, E., & Tuikka, T. (2022). An Organizational Maturity Model forData Spaces: A Data Sharing Wheel Approach. In *Data Spaces* (pp. 21–42). Springer International Publishing Cham.
DAMA International. (2009). The DAMA Guide to The Data Management Body of Knowledge. *Technics Publications, LLC Post*, 406.
de Bruin, T., Rosemann, M., Freeze, R., & Kulkarni, U. (2005). Understanding the main phases of developing a maturity assessment model. *ACIS 2005 Proceedings*, 8–19.
De Prieelle, F., De Reuver, M., & Rezaei, J. (2020). The Role of Ecosystem Data Governance in Adoption of Data Platforms by Internet-of-Things Data Providers: Case of Dutch Horticulture Industry. *IEEE Transactions on Engineering Management*, *69*(4), 1–11.
IBM. (2007). The IBM Data Governance Council Maturity Model : Building a roadmap for effective data governance. *Governance An International Journal Of Policy And Administration*, *October*, 1–16.
Jagals, M., & Karger, E. (2021). Inter-organisational data governance: A literature review. *Twenty-Ninth European Conference on Information Systems*, *June*, 1–19. https://aisel.aisnet.org/ecis2021_rp/57
Jussen, I., Schweihoff, J., Dahms, V., Möller, F., & Otto, B. (2023). Data Sharing Fundamentals: Definition and Characteristics Ilka. *HICSS 2023 Proceedings*.
Khatri, V., & Brown, C. V. (2010). Designing data governance. *Communications of the ACM*, *53*(1), 148–152.
Klein, H. K., & Myers, M. D. (1999). A set of principles for conducting and evaluating interpretive field studies in information systems. *MIS Quarterly: Management Information Systems*, *23*(1), 67–94.
Lee, S. U., Zhu, L., & Jeffery, R. (2017). Data governance for platform ecosystems: Critical factors and the state of practice. *PACIS 2017 Proceedings*.
Lis, D., & Otto, B. (2020). Data governance in data ecosystems - Insights from organizations. *26th Americas Conference on Information Systems, AMCIS 2020*, 0–10.
Lis, D., & Otto, B. (2021). Towards a taxonomy of ecosystem data governance. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2020-Janua*, 6067–6076.
Marcelo, M. I., Barros Lima, G. de F., & Farias Lóscio, B. (2019). Investigations into Data Ecosystems: a systematic mapping study. *Knowledge and Information Systems*, *61*(2), 589–630.
Merkus, J., Helms, R., & Kusters, R. (2021). *Data Governance Capabilities: Maturity Model Design with Generic Capabilities Reference Model*. *November*, 102–109.
Myers, M. D., & Newman, M. (2007). The qualitative interview in IS research: Examining the craft. *Information and Organization*, *17*(1), 2–26.
Nielsen, O. B., Persson, J. S., & Madsen, S. (2019). Why governing data is difficult: Findings from Danish local government. *IFIP Advances in Information and Communication Technology*, *533*, 15–29.
Panian, Z. (2010). Some practical experiences in data governance. *World Academy of Science, Engineering and Technology*, *38*(1), 150–157.
Rasouli, M. R., Trienekens, J. J. M., Kusters, R. J., & Grefen, P. W. P. J. (2016). Information governance requirements in dynamic business networking. *Industrial Management and Data Systems*, *116*(7), 1356–1379.
Rivera, S., Loarte, N., Raymundo, C., & Dominguez, F. (2017). Data governance maturity model for micro financial organizations in Peru. *ICEIS 2017 Proceedings*, *3*, 203–214.
The Open Group. (2018). ArchiMate® 3.1 Specification. In *The TOGAF® Standard, Version 9.2*. https://pubs.opengroup.org/architecture/togaf9-doc/arch/
TM Forum. (2022). *TM Forum Data Governance Guidebook*. https://www.tmforum.org/resources/standard/gb1023-data-governance-guide-book-v3-0-0/
Webster, J., & Watson, R. T. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. *MIS Quarterly*, *26*(2), xiii–xxiii.
Winter, J. S., & Davidson, E. (2019). Big data governance of personal health information and challenges to contextual integrity. *Information Society*, *35*(1), 36–51.
Yin, R. K. (2009). How to do better case studies. *The SAGE Handbook of Applied Social Research Methods*, *2*(254–282).
Zhang, J., Chen, B., Zhao, Y., Cheng, X., & Hu, F. (2018). Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues. *IEEE Access*, *6*, 18209–18237.