



Larissa Galdino de Magalhães Santos

ILDA



IDRC · CRDI

International Development Research Centre
Centre de recherches pour le développement international

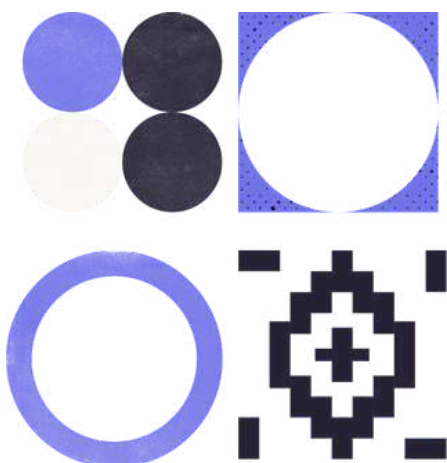
Canada



We are especially grateful to **Larissa Galdino de Magalhães Santos**, who carried out the research that underpins this report.

Larissa Galdino de Magalhães Santos is a specialist in digital governance, GovTech and responsible artificial intelligence. She has worked with prestigious organisations such as the United Nations University, the Global Center on AI Governance and the Getúlio Vargas Foundation, where she has led projects on digital transformation, open data and ethics in artificial intelligence. She is currently a Marie Skłodowska-Curie Fellow at the University of Bremen, where she develops strategies to improve GovTech ecosystems in European cities. With more than 15 years of research experience and a PhD in Political Science, Larissa brings extensive knowledge of the intersection between technology, governance and public policy.

This report was produced within the framework of the *Inter-American Programme for Data and Algorithms*, funded by the International Development Research Centre (IDRC).



**Author:**

Larissa Galdino de Magalhães Santos

PhD in Political Science – Unicamp

Marie Curie Fellow – Faculty 3 – University of Bremen, Germany

CyberBRICS Fellow – Law School – Fundação Getúlio Vargas, Brazil

Legal overview:

Juliana Almeida, Ana Carolina Cesar and Lara Salgueiro of KLA Advogados, via the connection facilitated by TrustLaw, the global legal pro bono network of the Thomson Reuters Foundation, through a partnership with the Patrick J. McGovern Foundation.

The contents of the legal overview reflect the views of Latin American Open Data Initiative (ILDA) and should not be taken to reflect the views of KLA Advogados, the lawyers who contributed, the Patrick J. McGovern Foundation, or Thomson Reuters Foundation. Similarly, KLA Advogados, the Patrick J. McGovern Foundation, and Thomson Reuters Foundation accept no liability or responsibility for actions taken or not taken or any losses arising from reliance on this report or any inaccuracies herein.

Coordination:

Gloria Guerrero

Design:

Violeta Belver

Style:

Aremí González

Acknowledgements:

International Development Research Centre (IDRC)

Translation facilitated by TrustLaw, supported by the Thomson Reuters Foundation, through a partnership with the Patrick J. McGovern Foundation



Index

Index.....	4
Foreword.....	5
Executive summary.....	7
Scope of the report.....	9
Data governance cycles in the Brazilian public sector.....	10
1. Data governance policies and strategies in Brazil.....	12
1.1 Centralised management and restrictive regulation of public information.....	12
1.2 Decentralised data management and regulation based on access to information and the open data infrastructure.....	13
1.3 New public management paradigm: governance and data sharing framework.....	13
1.4 Sustainable data governance: data infrastructures and data commons.....	14
2. Regulatory framework for data governance.....	14
2.1 Restrictive regulation of public information based on secrecy as a norm.....	16
2.2 Transparency and the right to public information as a constitutional principle.....	16
2.3 Legal framework for data sharing, privacy issues, data protection, transparency and state oversight.....	16
2.4 Strategic exchange, interoperability, security, privacy and protection of data.....	17
3. Coordination, implementation and capabilities of data governance.....	18
3.1. Management of Public Information and centralised resources.....	20
3.1.1 Decentralisation of information and resource management.....	20
3.1.2 Towards data management and governance: a data sharing scheme.....	20
3.1.3 Coordinated mechanisms for the responsible implementation of data governance: foundational capacities.....	21
3.2 Data Ecosystem in the Federal Public Administration.....	21
3.3 Data Governance Structure.....	22
3.4 Institutions for coordination, implementation and control of Data Governance.....	25
3.4.1 General Data Governance Coordination.....	25
3.4.2 Central Data Governance Committee (CCGD).....	26
3.4.3 Digital Government Secretariat.....	26
3.4.4 Office of the Comptroller General of the Union.....	26
3.4.5 Court of Auditors of the Union.....	27
3.4.6 National Data Protection Authority.....	27
3.5 Data Governance Resources and Capacities.....	28
3.5.1 New Database Catalogue.....	29
3.5.2 Reference Registries.....	31
3.5.3 Interoperability.....	31
3.5.3.1 Technological environments: Conecta Br Programme and Government APIs.....	31
3.5.4 Data Maturity Model.....	31
3.5.5 Data Governance Roadmap.....	33
3.5.6 Data Governance Forum: knowledge, control and social participation.....	34
4. Cases of data sharing.....	35
4.1 Data governance and solutions policy for the Government Electricity Agency.....	35
4.2 Financial authority and currency control governance policy.....	36
4.3 The Government Telecommunications Agency's Data Governance Policy.....	38
4.4 Data and Infrastructure Policy Information Committee.....	39
5. Challenges and recommendations.....	40
References.....	42
Annex: Legislative landscape.....	45



1. Introduction.....	45
2. What is the current legal framework, including laws, regulations, strategies and public policies, regarding the use, collection and processing of data in Brazil?.....	46
3. Challenges and opportunities related to data sharing in Brazil.....	47
4. Conclusion.....	48



Foreword

By: Gloria Guerrero

Executive Director of ILDA

In a deeply interconnected and increasingly digital world, data sharing and data governance are essential for meeting the challenges of the 21st century. In Latin America, these dynamics are influenced by unique contexts that combine promising developments and persistent challenges.

According to the first edition of the *Global Data Barometer*, Latin America faces fragmentation in its data policies: while some countries have made significant progress in openness and data protection, data sharing is still a work in progress.

For this project, data sharing is used in a broad sense, encompassing the regulatory frameworks that establish the technical and organisational guidelines for data sharing, institutional capacities, and political willingness to allocate resources and processes to enable these policies to succeed. In this way, data sharing and interoperability processes have a technical component linked to the creation of skills and their implementation, but also a political component relating to the decision to apply the policy and the cultural change within organisations that is also needed. We therefore consider the processes, people and systems that ensure that these policies remain in place over time.

It is within this context that the Latin American Open Data Initiative (Iniciativa Latinoamericana por los Datos Abiertos, ILDA) has conducted the research entitled “Data Sharing Strategies in Latin America”, which consists of three national case studies. This project is part of the *Inter-American Programme for Data and Algorithms* supported by the International Development Research Centre (IDRC), which seeks to explore the topic in greater depth. The purpose of this research project is to analyse and understand how data sharing systems work at a national level in Brazil, Colombia and Uruguay. These three case studies have allowed us to identify a set of best practices that can be inspirational for other countries in the region and to pinpoint challenges and areas of opportunity for this field of study.

Each case study seeks to understand the regulatory frameworks, data infrastructure and its characteristics, processes and implementation, and the involvement of various actors (public, private and civil society) in these data sharing processes at a national/federal level. This research follows on from a series of [Data Governance Reports carried out in Colombia, Mexico and Uruguay in 2022](#) and is complemented by a series of legal studies on data sharing conducted by specialised law firms in each country, which contributed on a pro bono basis through the connection facilitated by TrustLaw, the Thomson Reuters Foundation’s global legal pro bono network.

The project aims to provide a diagnosis and possible next steps on data governance, which could also be a useful input for future artificial intelligence (AI) governance in the region. This work aims not only to understand the existing regulatory and technical structures, but also to lay



the foundations for a sustainable, inclusive and democratic ecosystem that promotes interoperability and the ethical use of data-driven technologies.

The case of Brazil is presented below, led by Dr Larissa Magalhães and the law firm KLA Advogados. From the evolution of its regulatory frameworks towards a more collaborative and decentralised approach to the construction of a national data infrastructure, Brazil is leading the region in terms of the implementation of public policies that strengthen its data management ecosystem. Its efforts demonstrate how the combination of strategic investment in digital skills, data governance and the promotion of innovation can strengthen public services, catalyse economic development and respond to the needs that new technologies demand. However, there continue to be challenges. Structural inequalities and digital divides in Brazil underline the need for an approach that is not only technically robust but also puts human rights and equity at the centre of the discussion.

With this case study, ILDA reaffirms its commitment to contribute to the development of the regional data ecosystem and generate evidence to strengthen the existing data governance models and capacities. Brazil's experience, like that of the other countries explored in this project, is a reminder that making progress in democratic data governance is not a destination but an ongoing process that requires collaboration, vision and shared responsibility.



Executive summary

Data governance and data sharing in the public sector are key concepts to ensure efficiency, transparency and accountability in public administration. This report is part of the studies on **Data Sharing Strategies in Latin America of the Inter-American Data and Algorithms Programme** promoted by the **Latin American Open Data Initiative** (Iniciativa Latinoamericana por los Datos Abiertos, ILDA) and partners.

This executive summary presents an overview of data governance in the Brazilian public sector, specifically in the Federal Public Administration, addressing the scope of initiatives and the main findings and recommendations. In Brazil, the data governance framework encompasses a set of guidelines associated with government-to-government data sharing rules and the objectives of digital public service delivery and public policy advocacy. Data sharing between the government and third parties, between companies and the government or between companies and companies is regulated in accordance with the guidelines on personal data protection, consent and purpose. Therefore, data governance in Brazil includes the premises of data sharing.

Governança de dados

É o exercício de autoridade e controle que permite o gerenciamento de dados sob as perspectivas do compartilhamento, da arquitetura, da segurança, da qualidade, da operação e de outros aspectos tecnológicos. O compartilhamento de dados é a disponibilização de dados pelo seu gestor para determinado recebedor de dados.

Brasil. DECRETO Nº 10.046, DE 9 DE OUTUBRO DE 2019

According to the OECD, data governance refers to the technical, political and regulatory structures that facilitate the management of data from its creation and maintenance to disposal, across all areas of public policy. Data sharing is a crucial factor in maximising the benefits of data, facilitating access, sharing, collaboration and leveraging data sources to promote public sector-based innovations.

Governance also relates to the exercise of authority and control over data, as well as collaboration between the organisations and individuals that make up an ecosystem. Therefore, understanding and discussing governance implies a multi-organisational scenario, whose structures, including data sharing, must ensure reliability, security and compliance with regulations, including data protection.



It is well known that data governance is increasingly taking into account responsibility for the entire lifecycle of data and artificial intelligence applications among public sector organisations. In practice, however, there is still a long way to go before artificial intelligence is adopted in the public sector. Artificial intelligence applications rely heavily on data, and as data comes from a variety of sources, sharing and integrating it across government departments remains a challenge. In addition, the potentially isolated nature of IT systems implies a misalignment of data governance protocols, i.e. an interoperability gap that creates interrelated data security challenges.

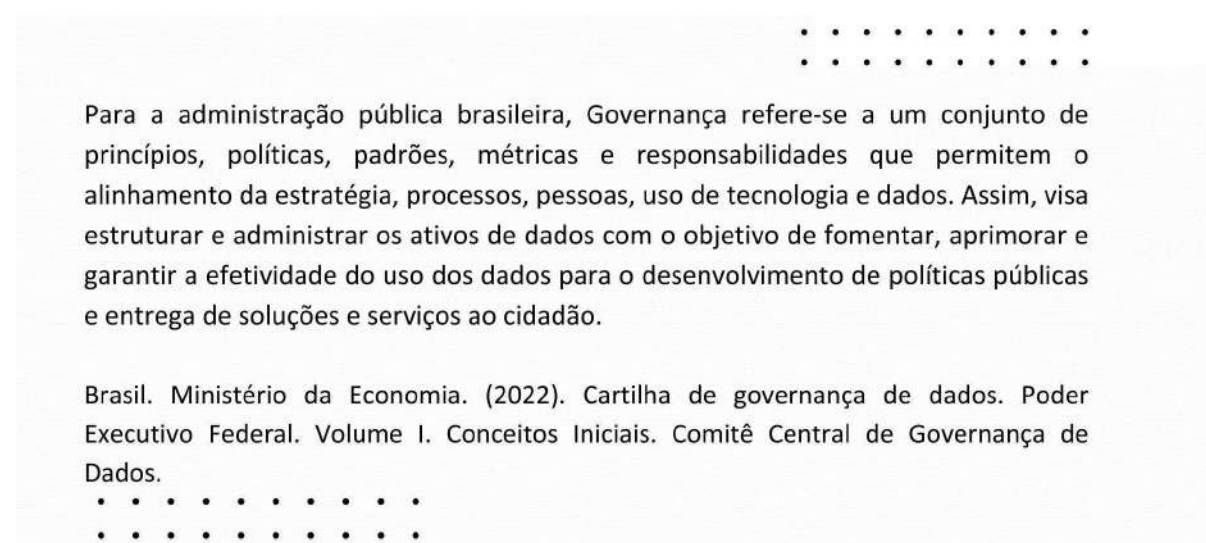
This report is therefore based on the perspective that data governance focuses on more than just the data, including also the social, technical and organisational resources involved in the collection, management, processing and use of data within ecosystems in which the public sector participates.

This expanded vision of governance is based on the perspective of data commons.¹ Data commons are communities that collectively and sustainably govern data and their relationships. By definition, data are related to groups and are involved in various activities amalgamated by governance.

Brazil has a long history of data collection, storage, processing and management, and data governance and sharing have been institutionalised in recent years. This has not been a uniform trajectory, as it has been guided by the government's fiscal, democratic, managerial and digital reforms.

Moreover, Brazil has an emerging data governance approach with the National Data Infrastructure and recommendations for its adoption at state and municipal level. Government-to-government data sharing is crystallising as a power to simplify and modernise public services, putting the citizen at the centre of initiatives, as well as data-driven decision-making and cost reduction.

The country has recently taken a step forward, including the strategic objective of launching a Data Governance Policy associated with investments in the National Data Infrastructure and data cataloguing as a fundamental premise to lead the actions of the Artificial Intelligence Plan.



¹ van Maanen, G. & Ducuing, C. & Fia, T. (2024). Data commons. Internet Policy Review, 13(2). <https://doi.org/10.14763/2024.2.1748>



Scope of the report

This report is part of the research on Data Sharing Strategies in Latin America of the Inter-American Data and Algorithms Programme promoted by the Latin American Open Data Initiative (Iniciativa Latinoamericana por los Datos Abiertos, ILDA) and its partners. The scope of this project includes an analysis of the current state of data governance in Brazil, with a special focus on data sharing.

This research included a review of strategies and policies, the regulatory framework, training practices, processes and implementation, stakeholder involvement and partnerships, identification of success stories and challenges faced by the public sector. It covers follow-up on the activities of the Data Governance Forum and Committee, as well as events and interviews with the decision-makers involved, from the National Open Data Infrastructure to the National Data Protection Authority.

The report also presents examples of good practice for sustainable, inclusive and accountable governance and exchange structures. The methodology used consisted of documentary analysis of official records and documents from the federal government and Brazilian states, interviews with stakeholders and a review of the literature on data governance, data protection, and information and technology systems in the Brazilian public sector. Finally, a list of recommendations suggests further steps for data governance to embrace the entire public data ecosystem in Brazil.



Main findings

Data governance cycles in the Brazilian public sector

The **First Cycle** is characterised by centralised management and restrictive data regulation. Management was based on the creation of the Federal Data Processing Service for strategic sectors and the Information Technology Enterprise for Social Protection. With the creation of public enterprises, the government's technological infrastructure was established. The legislation was based on the National Tax Code and the prohibition of disclosure.

The **Second Cycle** refers to decentralised data management and data regulation based on classification and access to information. With the e-Government Programme in place since 2000, the government has joined efforts to use information and communications technologies in the processes and delivery of public services. In this cycle, a proper approach to data governance was not yet in place. However, significant changes have been implemented through mandatory mechanisms for passive transparency and public information activities. The regulation of public information is no longer based on secrecy, but favours transparency, participation, collaboration and public integrity. The government's efforts to provide open data are complemented by the National Open Data Infrastructure and the consolidation of e-Government regulations and interoperability.

The **Third Cycle** is characterised by the emerging framework of data governance and data sharing resulting from the implementation of a new paradigm of public management and state–society relations. The Digital Governance Strategy established the sharing and integration of data, processes, systems, services and infrastructure as a goal for enabling public services. Subsequently, government decrees established the conditions for sharing databases and the creation of the Governance Committee to unify databases in the federal public administration. With the consolidation of the Civil Internet Framework and the General Data Protection Law, conflicts have arisen over the suitability of data processing, including personal data, and the exchange of citizens' data. In addition, the centralised structure of the Data Governance Committee has been subject to interventions from the Supreme Court in defence of citizens' rights and data use. Although data protection has been adopted as a constitutional right, data sharing still lacks the involvement of public sector agencies and entities in adhering to the premises of interoperability, business process culture, privacy, protection and security.

Currently, the **Fourth Cycle** is based on the establishment of a data governance structure within a National Public Data Infrastructure, with the objective of creating a policy framework for dealing with data in the public sector. The infrastructure conceptually functions as a set of rules, policies, architectures, standards, technological tools, information assets and human talent involving various agencies and entities connected by governance. Federally-led data governance aims to support the delivery of simplified public services, promote data-driven public policy decision-making, foster transparency in data use, and encourage the responsible use of data for long-term artificial intelligence. The infrastructure is designed to support the purposes of the entire data ecosystem. For this reason, the data governance structure already operates at the inter-organisational level, through management, standardisation and control bodies. Although an inter-organisational approach is not yet planned in the Federal Public Administration, the creation of a data policy allows for the secure, reliable and sustainable sharing, processing and



governance of data internally within the institutions. To further these objectives, the Central Data Governance Committee, together with the Digital Government Secretariat, has created a Database Cataloguing project establishing references for information protected by the public sector and a data maturity assessment to spread awareness and prepare organisations to build their own data governance. Consolidating the premises of the National Data Infrastructure is a strategic challenge for the current government.



1. Data governance policies and strategies in Brazil

There is no specific national strategy for data governance in Brazil. The Central Data Governance Committee, established by Decree No. 10,046/2019, is responsible for defining guidelines and guiding data sharing. The Committee also promotes forums and training to foster a culture of data governance. The Committee is preparing a policy to support governance at the level of bodies and entities of the federal public administration, enabling data sharing and ensuring the sustainability of the National Data Infrastructure.

The evolution of data governance policies and strategies in Brazil is marked by the State's management of information technologies and by reforms to modernise the public sector with the aim of simplifying public services and making them more efficient. Centralised public information management during the military period evolved towards decentralisation of information driven by technological development and government management reforms in the late 1990s.

Decentralised data management has been maintained through the government's new information architecture, based on e-government, the creation of service portals and the establishment of processes based on rules, standards and interoperability. The data vision is also driven by the policy of transparency, participation, collaboration and integrity called open government.

Efforts to accelerate digital transformation have resulted in the establishment of data governance to support the sharing of different infrastructures between government agencies and entities, to support the interoperability of systems for delivering services, and to better serve citizens using new information and communications technologies.

With the establishment of the governance framework, the government's recent intentions aim to strengthen the Data Governance Infrastructure based on interoperability, official governance bodies, the maturing of rules, standards and architectures, and the improvement of technological tools in favour of citizens and internal management. It also includes links with the bodies and entities of the Federal Public Administration.

1.1 Centralised management and restrictive regulation of public information.

Centralised management and state monopoly

- **Creation of Infrastructure and Public Enterprises:** Since the 1960s, Brazil began to introduce Information and Communications Technologies (ICTs) in the public sector with a centralised approach, in which the State, through public companies such as SERPRO and DATAPREV, monopolised data management and processing. This period was characterised by strong state control over the technological infrastructure, aimed at guaranteeing national sovereignty and information security, as well as promoting administrative efficiency.
- **Focus on Internal Efficiency:** During the 1970s and 1980s, the focus was on the automation of internal processes and the creation of databases to improve public management, mainly in areas such as financial and tax administration, with special attention to the digitisation of the tax declaration process.

Decentralisation and outsourcing



- **Reduction of Investment and Decentralisation:** With the tax crisis and the reduction of the State's investment capacity in the 1980s and 1990s, there was a delay in the technological upgrading of state-owned companies. This, coupled with pressure from the private sector and the emergence of new low-cost technologies, led to the decentralisation of ICT management, with each public body taking responsibility for its own technologies and information systems. Outsourcing of technology services also began to gain momentum.
- **Administrative Modernisation and e-Government:** The administrative reforms of the 1990s paved the way for the adoption of the e-government agenda, which began to take shape at the end of the decade. The creation of the Information Technology Resource Management System was an important step, but it remained focused on the coordination of IT resources, without directly addressing data governance.

1.2 Decentralised data management and regulation based on access to information and the open data infrastructure.

Extending e-Government and Interoperability Standards

- **Launch of e-Government:** With the formal launch of e-Government in 2000, Brazil began to implement a series of initiatives to improve the delivery of public services online. The creation of interoperability standards, such as e-PING, and accessibility standards, such as e-MAG, was crucial to ensure integration between different systems and the accessibility of services.
- **Challenges of Integration and Infrastructure:** Despite the progress made, the lack of an adequate infrastructure and the absence of full integration between the Federal Public Administration's corporate systems continued to present challenges. Public information management remained decentralised, with each agency retaining control over its own data and systems, without a unified data governance strategy.

Progress on Transparency and Data Governance Initiatives

- **Transparency and Open Government:** Brazil's accession to the Open Government Partnership in 2011 boosted the transparency and access to information agenda. The creation of the Transparency Portal and the Brazilian Open Data Portal were important milestones that allowed greater access to public data.
- **Start of Data Governance:** Although there was no unified data governance strategy until 2015, the standards and rules established by e-government, along with the creation of the National Open Data Infrastructure, began to outline a more structured approach to managing and sharing public data. However, data governance was still in an early stage and not yet fully consolidated.

1.3 New public management paradigm: governance and data sharing framework

- Since 2015, the concept of "e-government" has evolved into "digital government", which focuses on making public services more accessible and efficient for citizens. The 2016-2019 Multiannual Plan set out guidelines for improving governance, including information security and data sharing. The Digital Governance Policy, created by Decree No. 8638 of 2016, emphasised the use of technology for public service delivery and social participation. The Digital Governance Strategy (EGD, in Portuguese), launched in 2016, reinforced the importance of data sharing and interoperability between government systems, aiming to reduce costs and avoid duplication of efforts. Despite progress, data



sharing has faced criticism in relation to privacy and surveillance, and the Digital Transformation Strategy has not led to significant changes in data governance.

- Database Sharing Platforms: As of 2019, with the implementation of the Digital Governance Strategy (EGD), the Brazilian government has made significant progress in the integration and interoperability of databases between different public bodies. The EGD, outlined by the Digital Government Secretariat, emphasised the need to modernise public management through technology, prioritising the creation of platforms that facilitate secure and efficient data sharing between federal institutions. An important milestone in this process was the creation of *gov.br*, a unified platform that serves as a portal for various public services, centralising and simplifying access to government data and information.

1.4 Sustainable data governance: data infrastructures and data commons

- The National Digital Government Strategy: established as a priority by the Brazilian government, it aims to transform public administration through the use of digital technologies, with a focus on improving the efficiency, transparency and accessibility of public services. This strategy encompasses a series of actions to promote data sharing among public bodies, facilitating the interoperability of information and reducing bureaucracy. One of the main initiatives in this area is the development of integrated systems and digital platforms that allow different government agencies to access and use the same datasets, eliminating redundancies and increasing operational efficiency.
- The National Artificial Intelligence Plan (PNIA, in Portuguese): seeks to promote innovation and the ethical use of AI technologies in various sectors, including government. The PNIA foresees the creation of a favourable ecosystem for the development of AI solutions that can be applied to public management, notably by supporting the National Data Infrastructure and the Data Governance Policy. This includes improving government decision-making and the delivery of public services, always with careful attention to data protection and citizens' privacy.
- The Federal Digital Government Strategy (2024 to 2027) and institutionalisation of the National Data Infrastructure: establishes the creation of planning instruments for data governance and management associated with digital transformation plans. It defines the National Data Infrastructure as a set of rules to promote the strategic use of data held by public-sector organisations. The Digital Government Secretariat is responsible for promoting data governance and integration among federal entities.



2. Regulatory framework for data governance

The rules for collecting and storing public information in Brazil were initially driven by fiscal and taxation needs, as well as by social protection policies. The management of this information followed strict rules, especially in relation to data sharing, as provided for in the National Tax Code (CTN, in Portuguese) of 1966. Articles 198 and 199 of this code established tax secrecy as a priority, severely limiting data sharing between different public and private bodies.

Between 1965 and 1985, secrecy predominated in the Brazilian public administration, also influencing the rules on public information. Even with different approaches to different types of information, constitutions prior to the redemocratisation period did not guarantee the right of access to public information. With the enactment of the 1988 Constitution, based on the democratic rule of law, access to public information came to be considered a fundamental right.

²Restrictive data management gave way to the introduction of the principles of the right to public information, driven by the ideas of transparency and participation that permeated the scenario of the enactment of the Federal Constitution. Articles 5 and 216 of the Constitution established institutional rules: ensuring access and safeguarding secrecy when necessary, guided by necessity and collective interest; guaranteeing knowledge of information contained in government records or databases; document management and consultation of collective heritage by society; and, subsequently, access to or rectification of information recorded in databases of public bodies or institutions.

In the following years, the government issued several regulations concerning categories of public and confidential documents and the handling of confidential documents among public administration bodies. ³However, there were no significant changes in terms of regulating the right of access to information or data management, with no criteria for classifying information apart from the discretion of the classifier.

⁴The shift from opacity to transparency of public information began with the Fiscal Responsibility Law, which implemented transparency instruments for tax management through electronic disclosure. Discussions on the transparency of public information permeated the Transparency and Anti-Corruption Council at the level of the Office of the Comptroller General of the Union and the National Congress between 2009 and 2011, when the Access to Information Law was enacted. According to the Access to Information Law, information held by the State must be public, and access must be restricted only in specific cases. Access to public information thereby became the rule and secrecy the exception.

In the wake of the guidelines brought by the Access to Information Law, in 2014 the Civil Internet Framework incorporated rules relating to privacy and personal data protection for Internet users.

²BASTOS, C. R.; MARTINS, I. G. (Org.). *Comentarios sobre la Constitución brasileña* (Comments on the Brazilian Constitution). São Paulo: Saraiva, 1989.

³EPIK, M. *Derecho a la información: situación jurídica y desafíos* (Right to information: legal situation and challenges). Informática Pública, Belo Horizonte, v. 2, n. 2, p. 43-56, 2000.

⁴Complementary Law 101/2000, also known as the Fiscal Responsibility Law (LRF, in Portuguese), is an important milestone in Brazilian public finances. In general terms, it identifies ways to prevent and correct situations that endanger the balance of public accounts.



As of 2016, the Federal Public Administration regulations established new conditions for sharing public-sector databases with a view to streamlining and simplifying services.

Decree No. 8,789/16 intended to facilitate data transfer by means of a single legal basis for all data communication at the federal level. However, the decree does not establish limits to the cross-referencing of data between state agencies or transparency measures on data processing and it is limited to the publication of the databases by the respective agencies that maintain them.

In 2018, the General Data Protection Law (LGPD, in Portuguese) strengthened personal data protection and privacy measures, boosting the Brazilian system of data protection and access, especially with regard to the processing of personal data by public authorities. With the LGPD, the shortcomings of the security, protection and confidentiality rules and procedures of the legal framework relating to the exchange of databases have become even more worrying.

The new presidential decree No. 10,046 further increased the risks to citizens' privacy and data protection already identified. The decree created the Citizen Base Registry, organising sharing at various levels under the data manager, and it created the Central Data Governance Committee, whose discretionary and centralising power is contrary to the premises of the Brazilian system of data protection and access.

The growing tension between the legal basis of the data protection system and the legal basis of data sharing was reflected in the intervention of the Federal Supreme Court. In the face of speculation about unconstitutional state control over sensitive and personal data, the Court ruled that the exchange, cross-referencing and processing of data must comply with the purpose and practices of the LGPD, as well as with transparency measures. The Central Governance Committee also needed to be restructured, and provisions relating to the LGPD were added to the legal framework.

Currently, data governance is promoted through the National Data Infrastructure and the work of the Central Data Governance Committee and its resolutions. Data protection was recognised as a constitutional right in 2022. Moreover, the National Data Protection Authority has defined guidelines and requirements to be observed in the processes of personal data sharing by the government: formalisation and registration, object and purpose, legal basis, duration of processing, transparency and data subjects' rights, prevention and security.

In view of the expectations of the Federal Government's Data Governance Policy, agencies and entities are expected to adopt the principles and create their own rules to accommodate the specificities of the data and data sharing.

The regulatory evolution of data governance in the Brazilian federal public administration can be divided into four main periods, each of which represents a significant change in the way public information has been treated and regulated:

2.1 Restrictive regulation of public information based on secrecy as a norm

In this period, secrecy predominated in public administration, driven by fiscal and taxation needs and social protection policies. Regulation was strict, especially in relation to data sharing, as established in the 1966 National Tax Code. Fiscal secrecy was a priority, seriously limiting the exchange of information between public and private bodies, and the constitutions prior to redemocratisation did not guarantee access to public information.



2.2 Transparency and the right to public information as a constitutional principle

With the enactment of the 1988 Constitution, access to public information became a fundamental right, driven by the principles of transparency and participation. The articles of the Constitution guaranteed the right of access and safeguarded secrecy, when necessary, promoting a paradigm shift in the management of public data. However, the regulation of access to information continued to face challenges, with little change in practice and a lack of clear criteria for classifying information.

2.3 Legal framework for data sharing, privacy issues, data protection, transparency and state oversight

Since the Access to Information Law (2011), transparency has become the norm and secrecy the exception. This framework was complemented by the Civil Internet Framework (2014), which introduced internet privacy and data protection rules. Decree No. 8,789/16 simplified data sharing among government agencies and organisations but did not adequately address cross-referencing of data and transparency issues. With the enactment of the General Data Protection Law (LGPD) in 2018, the lack of clear criteria, especially in relation to privacy and security, for data sharing between government agencies and entities reinforced the need for regulation due to the exchange of personal data. The law provides for the exchange of personal data from one organisation to another, whether between organisations or between an organisation and a third party, for reasons such as the provision of services, business partnerships or even legal requirements.

However, Decree 10,046/19 expanded on the exchange of public data, creating categories, an official centralised body and an integrating base, the Citizen Base Registry. Risks related to data protection and privacy increased and the processes carried out by the Central Data Governance Committee lacked transparency, leading to the intervention of the Federal Supreme Court to align practices with the LGPD, provide transparency in data governance, and institute control mechanisms over the Citizen Base Registry and decentralise the composition of the official body.

2.4 Strategic exchange, interoperability, security, privacy and protection of data

The Digital Government Law added an interoperability layer to data governance. The aim of digitising government and increasing public efficiency was to ensure integrated action between agencies and entities through the exchange of data, including personal data, and the interoperability of data to eliminate unnecessary requirements for the delivery of public services.

The creation of the National Data Protection Authority (ANPD, in Portuguese) in 2022 and the enshrinement of data protection as a constitutional right have reinforced changes in the regulation of data governance. New changes in the regulatory framework for data governance have entailed important modifications, strengthening the requirements for data sharing by public authorities and emphasising transparency, security and data subjects' rights, as well as the role of the Governance Committee. Pending the Federal Government's Data Governance Policy and Regulation, agencies and entities are expected to adopt their own principles and rules to accommodate the specificities of data sharing in line with data protection best practices.



3. Coordination, implementation and capabilities of data governance

The creation of the Federal Data Processing Service (SERPRO) in 1964 was an initial milestone in the formation of a technological infrastructure that allowed information to be used more effectively in the formulation of public policy. In 1974, the creation of the Social Security Information and Technology Enterprise (DATAPREV) also expanded this infrastructure, improving the government's capacity to manage data, especially in the area of social protection.

The creation of public enterprises supported the centralised public information management model, and they were created to provide information and communications technology services. Although these enterprises were paid for providing services, there were no control, management or quality measures in place.⁵ Reduced investment in the sector, coupled with the rapid adoption of technologies, led to the exhaustion of the monopolistic and centralised model of information management.

Between the 1980s and 1990s, public information management began to be decentralised, allowing each government agency to take responsibility for its own IT services, resulting in large-scale outsourcing. In this context, data collection and storage policies started to be influenced mainly by fiscal, tax and social protection requirements, following public information management models similar to those of the private sector. However, data governance, which involves the management and control of data use and sharing, was not yet institutionalised, and initiatives focused more on the implementation of ICT systems than on an integrated approach to information governance.

⁶With the creation of the Executive Committee on Electronic Government (CEGE, in Portuguese) in October 2000, Brazil took decisive steps towards implementing e-government. Specific tasks were assigned to various public bodies to coordinate the implementation of measures and standards, creating the institutional environment required to establish e-government. In 2003, eight technical committees were created within the CEGE, responsible for planning and implementing projects in their respective areas. These committees, together with the CEGE, formulated policies and guidelines to guide e-government actions, notably the "E-Government Policy Proposal for the Federal Executive Branch", launched in September 2000, which defined the objectives until 2003.

The e-Government Programme was implemented under the coordination of the Presidency of the Republic, with the technical and management support of the Secretariat of Logistics and Information Technology (SLTI, in Portuguese) under the Ministry of Planning. The SLTI played a crucial role in strategic planning, inter-ministerial coordination and issuing IT-related standards. The institutional agreement combined the technical capacity of the SLTI with the political coordination capacity of the Presidency of the Republic, with the Head of the Civil House being the Chairman of the e-Government Committee and the Secretary for Logistics and Information Technology being responsible for the executive secretariat. Leadership of the programme in the ministries was generally exercised by the Executive Secretaries, and the Committee established

⁵DINIZ, V. *La historia del uso de la tecnología de la información en la gestión pública brasileña a través del CONIP – Congreso de Informática Pública* (The history of the use of information technology in Brazilian public management through the Congress of Public Information Technology). In: 10th INTERNATIONAL CONGRESS OF CLAD ON STATE AND PUBLIC ADMINISTRATION REFORM, 2005, Santiago. Annals... Chile, 2005.

⁶Diniz EH, Barbosa AF, Junqueira ARB, Prado O. *Gobierno electrónico en Brasil: una perspectiva histórica basada en un modelo de análisis estructurado* (e-Government in Brazil: a historical perspective based on a structured analysis model). *Rev Adm Pública* [Internet]. 2009 Jan;43(1):23-48. Available at: <https://doi.org/10.1590/S0034-76122009000100003>



mechanisms for monitoring and evaluating actions, such as weekly and bi-weekly meetings, as well as the participation of IT specialists to discuss more complex issues.

The e-Government Department strengthened the coordination and organisation of unified and integrated e-government actions, especially in the delivery of public services by electronic means. This department was responsible for standardising and disseminating the development of e-government actions, as well as for evaluating the programme's progress and proposing continuous improvements. During the first years, e-government in Brazil focused on three main fronts: interaction with citizens, improvement of internal government management, and integration with partners and providers, laying a solid foundation for the future of e-government in the country.

In 2005, the National Public Management and Debureaucratisation Programme (Gespública) was created to help improve the quality of public services provided to citizens and increase competitiveness as a result of continuous improvements in management. It was followed by the 2009 Citizens' Decree, which created the Citizen Service Charter and included a recommendation to improve information sharing to provide better services. Looking to the future, the government's main measures are aimed at implementing infrastructures and standards for integrated management through digitisation of processes.

⁷The government has created the Integrated System of Protocols to make it easier for citizens to track documents of interest to them online. The government also launched the Government Digital Identity to standardise agency portals. In 2015, the e-government paradigm focusing on the digitisation of internal processes evolved towards a digital government focusing on the relationship with citizens through the provision of simple, efficient and accessible services using digital technologies.

Since 2016, the government has implemented the Digital Governance Policy and the Digital Governance Strategy, guided by guidelines that prioritise digital self-service, ensuring access to information and social participation. The coordination and monitoring of actions related to digital governance are now carried out by the Ministry of Planning, Budget and Management, with the creation of committees and knowledge networks that foster collaboration among the different actors involved, including civil society. The strategy is aligned with the federal government's public policies and seeks to ensure efficiency and effectiveness in delivering services to citizens.

Within the framework of the data sharing, between 2016 and 2019, an official body was initiated to establish guidelines and oversee the Base Registry, the Central Data Governance Committee.

⁸The Special Secretariat for Debureaucratisation, Management and Digital Government (SEDGG, in Portuguese), under the Ministry of Economy (ME), was in charge of defining the procedure for building the catalogue to gather data under management, including data sharing. However, by virtue of a Direct Appeal of Unconstitutionality (ADI 6649) from the Supreme Court, the committee was restructured to comply with transparency measures. The control parameters and those relating to the General Data Protection Law were also respected.

Other strategies, policies and regulations drive the data governance approach associated with the use of digital technologies facilitated by interoperability of data between agencies to deliver public services to citizens: Digital Transformation Strategy, Digital Government Strategies, and Digital Government Law. In particular, the Digital Government Strategies (2020-2022 and

⁷Brazil. Ministry of Planning, Budget and Management. Secretariat for Logistics and Information Technology. Data standard, integration of Federal Government protocols: version 2.0 / Ministry of Planning, Budget and Management. Secretariat for Logistics and Information Technology, Ministry of Justice, National Archives. – Brasília: MP/SLTI, 2015.

⁸<https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/catalogo-de-bases-de-dados/catalogo-de-bases-de-dados>



2020-2023) set targets to promote the integration and interoperability of government databases, as well as creating references through the Base Registry. With the National Digital Government Strategy and the Brazilian Artificial Intelligence Plan, data governance has also become a strategic axis of the National Data Infrastructure. Therefore, recent actions relate to the implementation of data governance.

In addition to the government's regulatory and strategic inputs, the data governance structure established between 2016 and 2019 has changed as a result of the data protection and privacy system, information security measures, the composition of the data governance structure, including central and internal implementation and coordination, and the recent adoption and induction recommendations among the other federal entities. Data governance is now linked to the public data ecosystem and is part of the National Data Infrastructure. Data management and governance in the Federal Public Administration involves management, standardising, supervisory and official bodies.

The evolution of coordination, implementation and capabilities in data governance can be divided into four main periods:

3.1. Management of Public Information and centralised resources

With the creation of public enterprises, SERPRO and DATAPREV, both government information management and the technological infrastructure were centralised. These enterprises, which provide information and communications technology services, lacked effective quality management and control measures. Over time, lack of investment and rapid technological changes led to the eventual collapse of this centralised model, highlighting the need for a new approach to data governance in the federal government.

3.1.1 Decentralisation of information and resource management

Between the 1980s and 1990s, public information management underwent a process of decentralisation, with each government agency taking responsibility for its own IT systems, leading to the outsourcing of services. Data collection and storage policies started to be conditioned by fiscal, tax and social protection requirements, and practices similar to those in the private sector were adopted. However, information governance was not yet fully institutionalised, and initiatives focused mainly on implementing information and communications technology (ICT) systems, without an integrated approach to effective data management and sharing.

3.1.2 Towards data management and governance: a data sharing scheme

The creation of the Electronic Government Executive Committee (CEGE) represented an important milestone in the implementation of e-government in Brazil, promoting the coordination of actions and standards among various public bodies, including technical committees and guidelines for the development of e-government. The Secretariat for Logistics and Information Technology (SLTI), under the coordination of the Presidency of the Republic, played a central role in strategic planning and issuing standards. With the National Public Management and Debureaucratisation Programme (Gespública) and the Citizen Service Charter in 2009, the government focused on improving information sharing for the benefit of public services for citizens. In 2015, the transition to digital government reinforced expectations of data sharing as a central pillar for delivering more accessible services.

The implementation of the Digital Governance Policy and the Digital Governance Strategy in 2016 consolidated the objectives of digital self-service, social participation and access to information. Between 2016 and 2019, the data sharing framework was consolidated with the creation of the



Central Data Governance Committee, which is responsible for leading the guidelines on the Base Registry and the management of data sharing. The Special Secretariat for Debureaucratisation, Management and Digital Government defined the procedures for building the data catalogue. However, following a Direct Appeal of Unconstitutionality (ADI 6649) in the Federal Supreme Court, the committee was restructured to comply with transparency requirements and the parameters of the General Data Protection Law.

3.1.3 Coordinated mechanisms for the responsible implementation of data governance: foundational capacities

This phase is marked by the integration of various strategies and policies, such as the Digital Transformation Strategy, the Digital Government Strategies (2020-2022 and 2023-2024) and the Digital Government Law, which seek to strengthen interoperability among government databases. These initiatives also established new resources related to the Base Registry and enhanced data governance as a key element of the National Data Infrastructure, in line with the Brazilian Artificial Intelligence Plan. The data governance system was gradually improved to incorporate stronger data protection, privacy and information security guidelines for the entire public data ecosystem. Inter-organisational governance plays a crucial role in coordinating the implementation of data security and data processing requirements, both within and between agencies. An inter- and intra-agency governance structure has been promoted by the Digital Government Secretariat, the Data Infrastructure Directorate, the General Data Governance Coordination, the Central Data Governance Committee, and the control and inspection bodies to help achieve the institutional mission through coordinated governance mechanisms that facilitate the implementation of security requirements, data protection, data processing, risk mitigation and ethical use of data within the agencies.

Although there is a division of labour, the management bodies also participate in the activities of the official bodies and are connected to the data ecosystem through the National Data Infrastructure, providing training, maturity guidelines, references, protection mechanisms, privacy and interoperability. In practice, data governance resources and capabilities are being driven by all the agencies and organisations involved. It is expected that with the Data Cataloguing and Data Maturity projects, the other agencies and entities that make up the Federal Public Administration will adopt data governance internally.

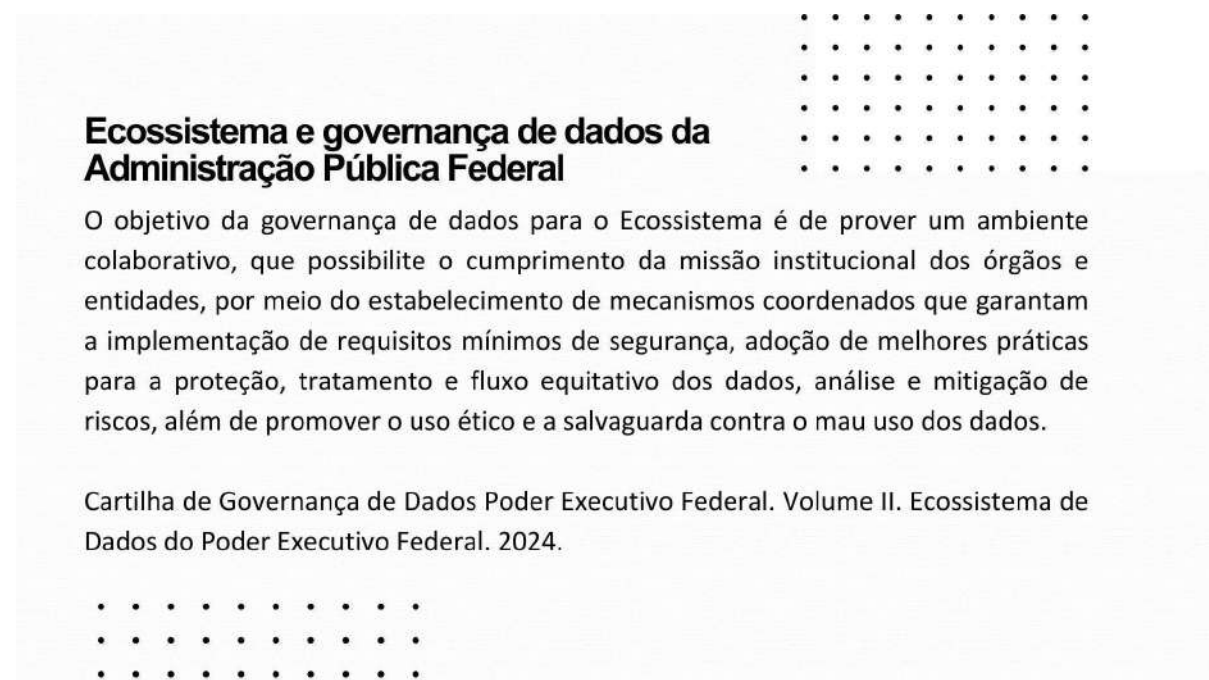
3.2 Data Ecosystem in the Federal Public Administration

Based on the premise of e-government, a data ecosystem was created in which the data protected by the administration is decentralised and managed according to the strategic management of each agency and type of public policy.

In the federal public administration, there is a wide variety of bodies, such as foundations, autonomous bodies, public enterprises, as well as ministries and agencies, which perform different functions and maintain different relationships among the bodies, with civil society and within the bodies themselves. In the government's view, each agency in the ecosystem needs to be involved through laws, standards and general policies, but also to define its data governance mission internally.



⁹To lead this ecosystem, the Brazilian government has a structure formed by institutions acting at an inter-organisational and intra-organisational level to align data governance, data management and data oversight across the ecosystem. At an inter-organisational level, the institutions act to coordinate general policies, laws and regulations. At an intra-organisational level, the agencies and entities act with the support of the institutions of the ecosystem to implement and execute data governance internally and in relation to others.

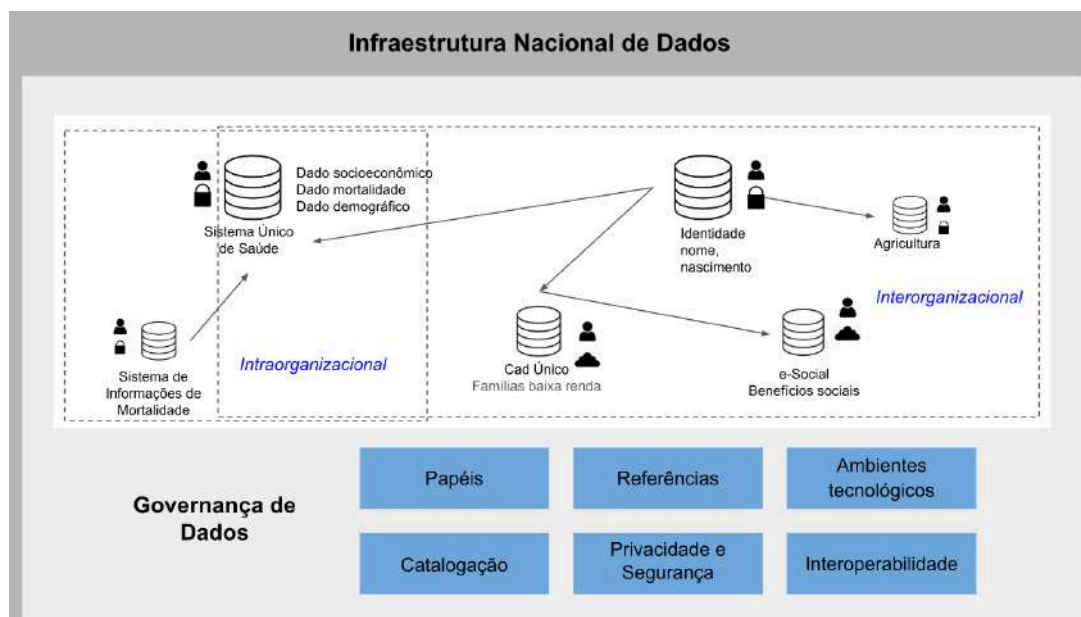


3.3 Data Governance Structure

In the context of governance, Figure 2, there is a structure that facilitates inter-organisational coordination – policies, rules, guidelines and management – and intra-organisational implementation, supported by the internal attributes of agencies and control instruments. While the IND is a conceptual approach that came about to support data governance in the government data ecosystem, the governance structure is based on the institutions that define data-related policies, laws, regulations, strategies and guidelines.

Figure 2: Data Governance in the context of the National Data Infrastructure

⁹Ministry of Service Management and Innovation. 2023. Data Governance Handbook. Central Data Governance Committee. Volume II. Data Ecosystem of the Federal Executive Branch. Public. Available at: <https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadedados/arquivos/CartilhadeGovernancadeDadosEcosistemadeDados.pdf>



Source: Adapted from the Central Data Governance Committee. Data Governance Week. Ministry of Public Service Management and Innovation. August 2024.

A data governance structure operates in the Federal Public Administration given the decentralised characteristics of the data ecosystem, both at agency and inter-agency level. **Inter-organisational governance among bodies helps achieve the institutional mission through coordinated mechanisms**, while **inter-organisational governance ensures the implementation of security requirements, data protection, data processing, risk mitigation and ethical use of data within agencies**. At the same time, **Data Governance is connected to the data ecosystem through the National Data Infrastructure**, as shown in Figure 2.

The Federal Government's Data Governance Structure, illustrated in Figure 3, consists of two pillars and control elements. The pillar of central governance focuses on data governance policies, regulations, standards and management. The pillar of internal governance focuses on actions relating to the implementation and execution of each body's own guidelines, defining functions, programmes and policies.¹⁰ The control elements consist of the bodies that monitor, recommend and establish adjustments in the broader sense of data governance, in the context of public policy and government management, complementing its coordination and implementation.

¹⁰Ministry of Service Management and Innovation. 2023. Data Governance Handbook. Federal Executive Branch, Central Data Governance Committee. Volume II. Data Ecosystem of the Federal Executive Branch. Public. Available at: <https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadados/arquivos/CartilhadeGovernancadeDadosEcossistemadeDados.pdf>



Figure 3: Data governance structure



Source: Adapted from the Central Data Governance Committee. Data Governance Week. Ministry of Public Service Management and Innovation. August 2024.

¹¹Each pillar is characterised by its relationship with agencies and actors, purpose, organisational resources, type of governance and governance instruments. The pillar of inter-organisational governance has the following characteristics:

Características da Governança Central	
Envolvimento	Envolve a coordenação entre órgãos, poderes, entidades, organizações internacionais, sociedade e mercado.
Propósito	- Criar mecanismos que promovam a colaboração entre essas diversas partes; - Facilitar o compartilhamento de dados, considerando acesso, uso e integridade; - Garantir que o uso dos dados siga uma proposta de valor.
Organização	A organização está relacionadas às características do ecossistema do governo. Atualmente, existe uma coordenação geral de governança de dados e um comitê executivo de governança de dados, e uma secretaria de gestão.
Abordagem	A governança é compartilhada entre os órgãos normatizadores, implementadores e fiscalizadores.
Instrumentos de Governança	- Comitê Central de Governança de Dados e Subcomitê - Fórum de Governança de Dados - Capacitação - Projetos

The pillar of inter-organisational governance has the following characteristics:

¹¹Ministry of Service Management and Innovation. 2023. Data Governance Booklet. Federal Executive Branch. Central Data Governance Committee. Volume II. Data Ecosystem of the Executive Branch Federal. Public. Available at: <https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadedados/arquivos/CartilhadeGovernancadeDadosEcossistemadeDados.pdf>



Características da Governança Interna	
Envolvimento	Envolve a coordenação interna no nível do órgão, respectivos departamentos/diretorias a fim de implementar e executar a governança de dados coordenadamente.
Propósito	- Estabelece estrutura organizacional de governança;; - Assegura o gerenciamento e uso de dados responsável; - Aplica os recursos de governança para melhorar os dados (qualidade e padronização).
Organização	A organização está ancorada na hierarquia de cada organização, e conforme estruturas internamente estabelecidas.
Abordagem	Cada órgão é autônomo para estabelecer a governança interna desde que siga as diretrizes centrais.
Instrumentos de Governança	Os instrumentos instituídos conforme cada órgão.

¹²In the longer term, with the establishment of the Data Governance Policy, it is expected that implementing agencies will be able to carry out more appropriate internal governance with their own strategies and policies, in line with central governance.

3.4 Institutions for coordination, implementation and control of Data Governance

3.4.1 General Data Governance Coordinator

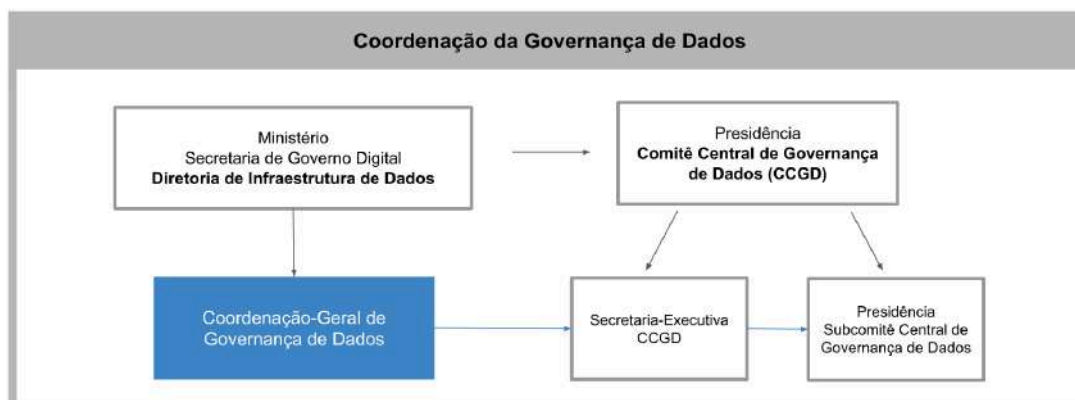
¹³The General Data Governance Coordinator works under the Public Data Infrastructure Directorate. The Coordinator acts through the Directorate/Department located in the Digital Government Secretariat to formulate data governance policies and guidelines, support data interoperability and sharing, develop and propose data models, processes, formats and standards, and lead data governance monitoring and evaluation tools.

The General Coordinator currently guides and oversees data governance through its main projects: Database Cataloguing and the Data Maturity Model. The General Data Governance Coordinator also has an important role in the Central Data Governance Committee, as it is the representative of the Executive Secretariat and Chair of the Data Governance Sub-Committee, as shown in Figure 4.

¹²Central Data Governance Committee. National Data Infrastructure. Information Technology Directorate of the Shared Services Secretariat. Data Governance Week 2024. Ministry of Public Service Management and Innovation. Available at: <https://www.youtube.com/watch?v=Fh4jgkzXujl>

¹³ <https://www.gov.br/gestao/pt-br/acesso-a-informacao/institucional/competencias/secretaria-de-governo-digital>

Figure 4: Role of the General Data Governance Coordinator



Source: Adapted from the 4th Meeting of the Data Governance Forum. Data Catalogue. Ministry of Public Service Management and Innovation. November 2023.

3.4.2 Central Data Governance Committee (CCGD)

The Central Data Governance Committee (CCGD, in Portuguese) was created by Decree No. 10,046 of 9 October 2019 with the task of providing advice on data governance policies and guidelines for direct, autonomous and foundational public administration bodies at the request of the Digital Government Secretariat (SGD, in Portuguese). The Committee is currently chaired by the Ministry of Public Service Management and Innovation and includes bodies such as the Civil House of the Presidency of the Republic, the Office of the Attorney General of the Union, the Office of the Comptroller General of the Union and the Special Secretariat of the Federal Revenue, among others, including two civil society organisations.

In June 2020, the CCGD created a Technical Subcommittee on Data Governance, which is responsible for proposing guidelines on how to structure data governance in the agencies mentioned in Decree No. 10,046/2019. This Subcommittee has representatives from the same agencies as the CCGD, as well as three additional agencies: the National Electricity Agency, the Ministry of Education and the National Foundation for the Development of Education, broadening the dialogue and collaboration among the different sectors of public administration.

3.4.3 Digital Government Secretariat

The Digital Government Secretariat (SGD, in Portuguese) plays a crucial role in data governance, promoting integration among government agencies and structures to eliminate data silos and improve public services for citizens. With the creation of the Central Data Governance Committee by Decree No. 10,046/2019, the SGD established guidelines for data sharing, security policies and quality assessment of the Citizen Base Registry. In addition, the SGD may consult the Committee regarding data governance issues.

The SGD also leads the Federal Executive Branch's Information Technology Resource Management System and is responsible for formulating and implementing policies and guidelines for IT management in the federal government. It also coordinates the National Digital Government Strategy in collaboration with states, municipalities and the Federal District.

The SGD is responsible for managing the Data Governance Forum.

3.4.4 Office of the Comptroller General of the Union

The Office of the Comptroller General of the Union (CGU, in Portuguese) acts as the main body responsible for the Federal Government's Transparency and Open Data policies. It is responsible



for coordinating and overseeing open data initiatives in the federal government, in accordance with the Open Data Policy Decree, as well as managing the Open Data Portal (dados.gov.br). The CGU also plays an essential role in reconciling the Access to Information Law with the General Personal Data Protection Law.

3.4.5 Court of Auditors of the Union

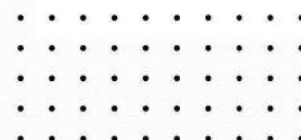
The Court of Audits of the Union (TCU, in Portuguese) is a control body external to the Brazilian government that is in charge of supervising and verifying the use of public resources and the conformity of the acts of the Federal Executive Branch, among other functions. The TCU plays a crucial role in promoting transparency, efficiency and accountability in the management of public data and resources.

3.4.6 National Data Protection Authority

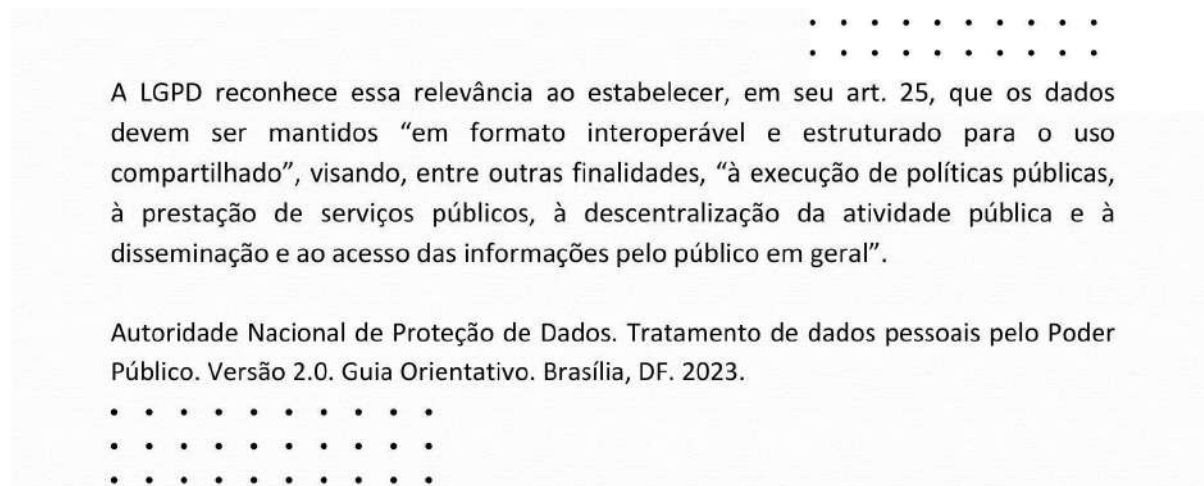
The General Data Protection Law created the National Data Protection Authority (ANPD, in Portuguese), an autonomous body linked to the Executive Branch that is in charge of ensuring compliance with the LGPD and applying sanctions in cases of infringement. The ANPD also draws up guidelines, advises the public on data protection practices and promotes adherence to the legislation by institutions handling personal data.

In addition to its supervisory functions, the ANPD promotes the regulation of data sharing, as defined by the LGPD, which allows the communication and transfer of data between public and private bodies. This use must respect the principles of the law, ensuring transparency and data subjects' rights when sharing data in the public sector. The LGPD also created the National Data Protection and Privacy Council, consisting of 23 members representing different sectors of society, to collaborate in the formulation of data protection policies. The objective of the ANPD is to enforce compliance with the rules and to ensure that data sharing takes place in a secure and transparent manner and in accordance with citizens' rights.

Compartilhamento de dados na visão da ANPD



De forma mais específica, a LGPD utiliza o termo “uso compartilhado de dados”, que é definido como a “comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados.”



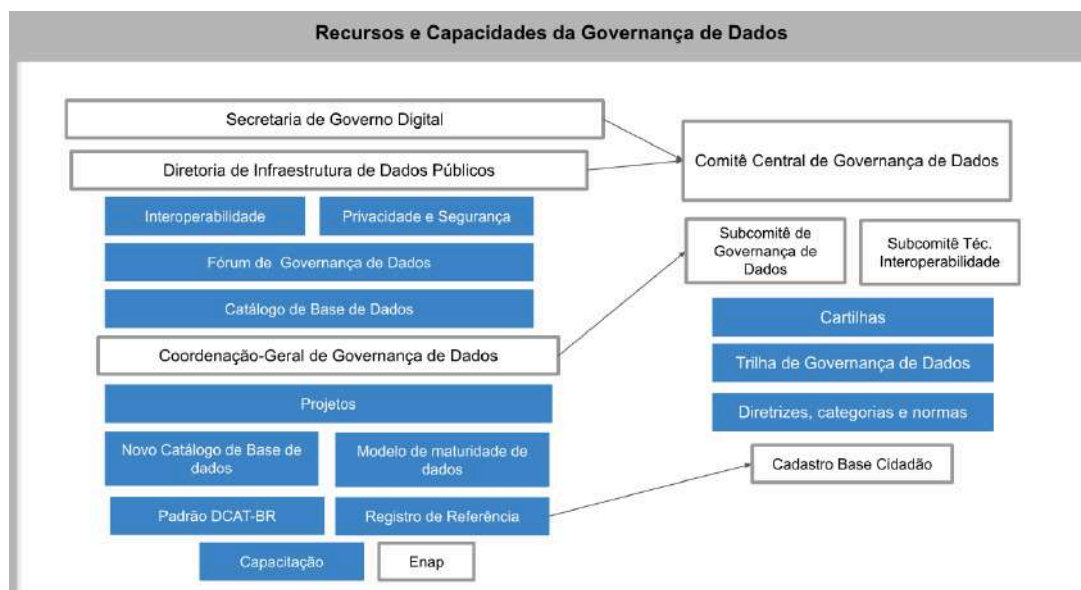
3.5 Data Governance Resources and Capacities

Data Governance resources and capabilities are distributed among the management and standardisation bodies as shown in Figure 5. The Digital Government Secretariat, the Public Data Infrastructure Directorate and the General Data Governance Coordination are responsible for projects, resources and training. The Digital Government Secretariat is responsible for the Public Data Infrastructure, which is coordinated by the Directorate. The Secretariat manages the interoperability, privacy and security resources of the Data Governance Forum and supports the Database Catalogue. The General Data Governance Coordination is involved in various National Infrastructure resources (see Figure 2), giving priority to assessment and management projects: the data maturity project and reference registries.

The official standardisation bodies, the Central Data Governance Committee and the Data Governance Sub-Committee, are responsible for the data ecosystem resources: the data governance roadmap and updates to the Citizen Base Registry through the reference registries.

Although there is a division of labour, the management bodies are involved in the activities of the official bodies – the Committee and the Sub-Committee – because the managers hold the positions of chairperson and executive secretary, as shown in Figure 4. In practice, therefore, there is no such a division of labour.

Figure 5: Organisational chart of resources and the capacity for data management and governance



Source: Adapted from the 4th Meeting of the Data Governance Forum. Data Catalogue. Ministry of Public Service Management and Innovation. November 2023.

3.5.1 New Database Catalogue

The Database Catalogue is a fundamental resource for data governance, as it allows the identification of government databases, their characteristics, where they are located and who the responsible custodians are. The Database Catalogue should not be confused with the Base Registry, which is an integrated database and serves as a reference base of information on citizens for federal government bodies and entities.

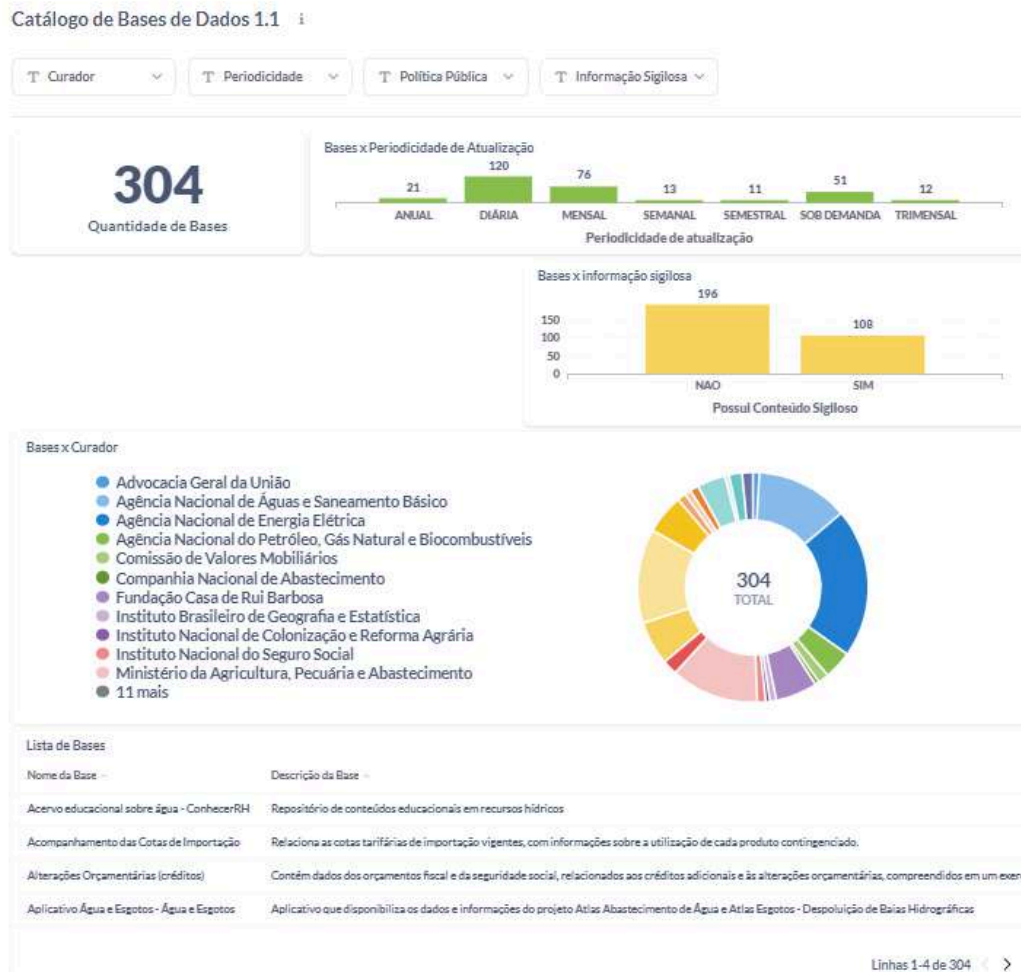
The Digital Government Secretariat, with the support of the Central Data Governance Committee, carries out a continuous process of compilation and review of the information in the catalogue. New criteria can be added and reviewed, and the Digital Government Secretariat (SGD) is in constant contact with the managers to ensure that the data are kept up to date. This update can be done mainly in two ways: through formatted spreadsheets or interviews.¹⁴

For organisations with up to five databases, updating can be done through interviews, which facilitates the collection of information. In cases where there are more than five databases, the data are reviewed and updated through spreadsheets submitted by the organisations. The new catalogue aims to centralise the metadata managed by public authorities, making it available in a simplified form via dashboards and a metadata portal linked to the government's Open Data Portal. The catalogue currently has an up-to-date dashboard with information on the databases, Figure 5.

¹⁴

<https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/catalogo-de-bases-de-dados/catalogo-de-bases-de-dados>

Figure 5: Database Catalogue Dashboard



Source: Database Catalogue v 1.1. National Data Infrastructure

¹⁵Moreover, there is a data cataloguing project led by the General Data Governance Coordinator, which also chairs the Central Committee's Data Governance Sub-Committee, covering a new cataloguing standard and the development of a metadata portal. The new cataloguing rule has already been launched for DCAT-Br. A centralised tool is being developed by the SGD, the directorates and the Office of the Comptroller General of the Union, which maintains the open data portal. ¹⁶The idea is to create the National Metadata Portal to integrate the different databases and facilitate policy implementation. A pilot case is underway. The project is based on the premise of data findability:

- Finding out what data exist in the federal public administration.
- Defining the data controller.
- Understanding the correct meaning of the data.
- Identifying possibilities for integration with other bases.
- Promoting transparency for the data subject.

¹⁵Central Data Governance Committee. National Data Infrastructure. Information Technology Directorate of the Shared Services Secretariat. Data Governance Week 2024

¹⁶4th Meeting of the Data Governance Forum. Data Catalogue. Ministry of Public Service Management and Innovation. November 2023.



3.5.2 Reference Registries

¹⁷Reference registries refer to information from the data sources of the respective federal government bodies and entities, thus functioning as a base registry. It is a database that synthesises a minimum dataset that provides interoperability and integration with other datasets of federal government bodies and entities.

The reference registry was established by the data sharing regulation and the Digital Government Law as a requirement for data interoperability, making its disclosure mandatory.

The objective of the creation of reference registries between government agencies and entities is to standardise the government dataset, support data management, promote consistency between data, eliminate ambiguities, promote legal certainty, promote transparency about the data held by the State and facilitate compliance with the General Data Protection Law.

The reference registries are established by resolutions of the Central Data Governance Committee. At least eight reference registries are currently in place:

- Address base registry
- Country reference registry
- Reference registry of federal executive branch officials
- Reference registry of the organisational structures of the federal executive branch
- Reference registry of public services portal
- Reference registry of persons with disabilities
- Military status reference registry

3.5.3 Interoperability

¹⁸The Digital Government Secretariat works together with the Central Data Governance Committee to promote, encourage and facilitate inter-agency interoperability through Conecta Br and government APIs. In addition to these platforms, interoperability links the data management body, which is responsible for making the data available in accordance with the sharing rules, and the data receiving body, which uses and is responsible for the data made available.

3.5.3.1 Technological environments: Conecta Br Programme and Government APIs

The Conecta gov.br programme aims to promote interoperability in the federal government so that citizens do not have to submit information that the government already has. Conecta is an initiative of the Secretariat of Digital Government for the bodies and entities of the Federal Executive Branch. The Catalogue of Government APIs brings together the main APIs available to public bodies. An API is a technology that allows a system to “talk” to another system without human intervention.

While Conecta gov.br promotes interoperability, the Catalogue of Government APIs brings together the main APIs that allow communication between public systems without manual intervention.

¹⁷<https://www.gov.br/governodigital/pt-br/IND/registros-de-referencia>

¹⁸ <https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/interoperabilidade>



3.5.4 Data Maturity Model

¹⁹The Data Maturity Model (MMD, in Portuguese) was developed by the Data Governance Sub-Committee with the aim of helping organisations to assess and improve their data governance practices. This Model provides a clear framework that allows federal institutions to analyse their level of maturity in various areas, such as policies, processes and the use of technologies related to data management.

Supported by the Digital Government Secretariat and developed by the Central Data Governance Committee, the MMD guides the bodies of the executive branch in implementing effective Data Governance Programmes. It is based on research that examines international maturity models with the aim of strengthening the data culture in public entities and maximising the strategic value of these assets.

The MMD indicates the following levels of maturity:

- 1st LEVEL – Not initiated: indicates the absence of the phase assessed.
- 2nd LEVEL – Initiated: presents an initiative or an ongoing project and/or plan.
- 3rd LEVEL – Emerging: has a project in progress, something more solid than an initiative.
- 4th LEVEL – Developed: processes already in place and management more robust; and
- 5th LEVEL – Optimised: automation, culture and improvement iterations clearly present.

The MMD not only provides a diagnosis of the current situation of organisations but also identifies opportunities for improvement through the Maturity Level Assessment. The MMD is a way of implementing data governance at an organisational level, i.e. it is a resource for intra-organisational governance.

The assessment system consists of 40 self-assessment questions with explanatory scenarios. In total, 12 topics are assessed according to maturity level: quality, usage, knowledge, ethics, artificial intelligence, data literacy, analytics, management, decision-making, open data, accountability and interoperability, as shown in Figure 6.

Figure 6: Data Maturity Model: assessment scheme



¹⁹Central Data Governance Committee (2024). Data Maturity. DATA MATURITY TECHNICAL GROUP. Technical Subcommittee on Data Governance. Digital Government Secretariat. Available at: <https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/maturidade-de-dados/arquivos/modelo-maturidade-de-dados-mmd.pdf>

Source: Central Data Governance Committee (2024). Data maturity. Technical Subcommittee on Data Governance.

With the results of the assessment, institutions can develop data strategies and define short-, medium- and long-term goals, as well as raising employee awareness of the importance of data as a valuable asset.

3.5.5 Data Governance Roadmap

The objective of the Data Governance Roadmap is to support the implementation of a data culture in the Federal Executive Branch based on current legislation and guidelines related to privacy, transparency, data protection, value creation, ethics, improvement of state performance and efficiency in the use of data for the benefit of citizens.

In addition, the Roadmap guides agencies on a journey that seeks to integrate infrastructure, regulation, the digital economy and people with social values into the management of government data, ensuring the protection of citizens' individual rights. The content will be organised in five thematic volumes, distributed according to the needs identified, as shown in Figure 7.

Two booklets have been published so far.²⁰The Booklet of Initial Concepts on data governance explains concepts related to data governance, the approach to data governance in the context of the Federal Public Administration, legislation, related initiatives, advantages and disadvantages of adopting data governance.

²¹The Federal Executive Branch's Data Ecosystem Booklet explains the premises of digital government and data, e.g. government as a data provider, government as a platform, smart government, and government as a regulator and provider. The Booklet also presents the management aspects of data governance, the bodies and entities involved, and the related organisational aspects.

Figure 7: Data Governance Roadmap Booklet



²⁰

<https://www.gov.br/governodigital/pt-br/governanca-de-dados/forum-governanca-de-dados/cartilha-de-governanca-de-dados-volume1-8-12.pdf>

²¹

<https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadedados/arquivos/CartilhadeGovernancadeDadosEcosistemadeDados.pdf>



Source: Data Governance. Data Governance Roadmap (2024). Available at: <https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadedados>

The next editions planned are as follows:

- Volume 3 – Roles and responsibilities of the Federal Executive Branch regarding Data Governance.
- Volume 4 – Data Governance Platforms in the Federal Executive Branch.
- Volume 5 – Practical Actions for implementing a Data Governance Programme.

3.5.6 Data Governance Forum: knowledge, control and social participation

²²The Data Governance Forum was created by the Digital Government Secretariat as a space for exchange of experiences and learning on data governance in the public sector. The Forum was officially launched in 2022 with the broadcasting of the meetings on the YouTube channel of the Ministry of Management and Innovation.

Organisationally, the Forum has become a space for social participation in data governance in the federal public administration, with a growing number of participations, chats and WhatsApp groups open to the public. In total, five meetings have been held. The sixth meeting of the Forum was renamed the Public Data Infrastructure Forum.

The first meeting, held in December 2022, presented the premises of the Forum and promoted the launch of the Data Governance Booklet.

- 1st Meeting of the Data Governance Forum

Held in December 2022, it brought together approximately 300 participants. The virtual event saw the presentation of the first volume of the Federal Executive's Data Governance Booklet, which contains the initial guidelines for establishing policies and directives with a focus on improving integrated services. This volume is part of a series of publications aimed at strengthening the data culture in federal institutions through the Data Governance Roadmap.

- 2nd Meeting of the Data Governance Forum

Meeting held in March 2023 on Data Governance Policy. The event, which was held virtually, was attended by nearly 1,000 people and aimed to promote a data culture in the 251 bodies that make up the Information Technology Resource Management System (SISP, in Portuguese), as well as to discuss problems, needs, solutions and risks faced by the institutions.

Representatives of the Office of the Comptroller General of the Union, the Office of the Attorney General of the Union and the National Electricity Agency participated in this year's round table. According to the Digital Government Secretariat, the meetings are essential for building an integrated policy in the public sector, listening to those who are directly involved in the creation and management of data governance. They underlined that it is essential to give citizens the conditions to exercise their rights and stressed the importance of cooperation between the bodies.

- 3rd Meeting of the Data Governance Forum

²²For information about the Forum, presentations and access to meetings, see: <https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadedados/forum-de-governanca-de-dados> Accessed in September 2024.



Meeting held in June 2023 on the Data Governance Maturity Index. Representatives from the National Treasury Secretariat, Petrobras and Banco do Brasil shared the tools and strategies used to assess internal data governance maturity. The event was attended by approximately 900 people.

- 4th Meeting of the Data Governance Forum

Meeting held in November 2023 to discuss the topic of Data Catalogues. Public servants involved in the governance policies of government bodies such as the Central Bank of Brazil, the National Telecommunications Agency and the National Electric Energy Agency were invited to show the tools and strategies they use to build their data catalogues.

- 5th Meeting of the Data Governance Forum

Meeting held in April 2024 focusing on data strategies in Latin America. Representatives of the Agency for e-Government and the Information and Knowledge Society of Uruguay and the Digital Development Directorate of the National Planning Department of Colombia participated in the Forum, presenting their experiences. The Digital Government Secretariat presented the Brazilian proposal for data infrastructure.

- 6th Meeting of the National Data Infrastructures Forum

The meeting was held in August 2024 with a new topic on the National Data Infrastructure. With the new conceptual design of the public data ecosystem, new speakers from municipal and state initiatives were invited to discuss their experiences. Recife City Council presented a proposal for a city council data strategy, with the idea of unifying data from all the channels on a unified platform called Farol. The Information Technology Company of the State of Minas Gerais presented Data Lake MG, a tool that allows the unification of public safety information in a single data repository.

²³In addition to the Forum, August 2024 saw the Data Governance Week, hosted by the Ministry of Public Service Management and Innovation and organised by the IT Directorate of the Shared Services Secretariat under the Digital Governance and Information Security Committee.

4. Cases of data sharing

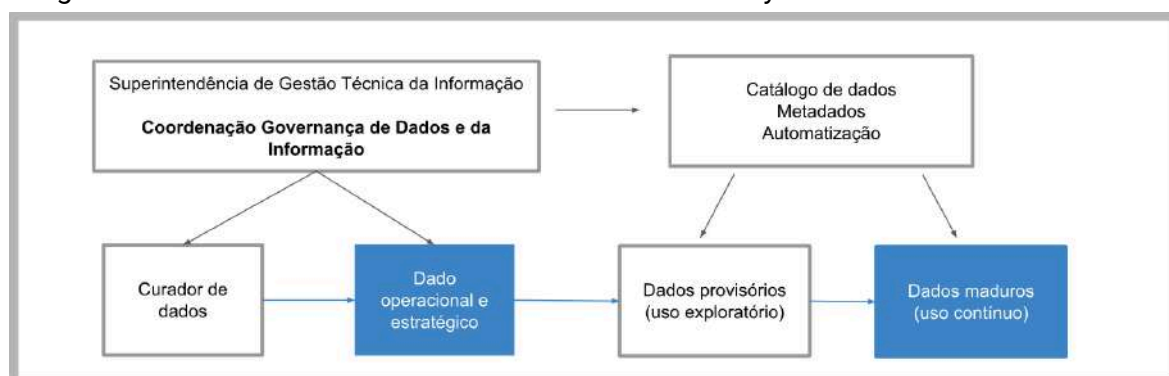
4.1 Data governance and solutions policy for the Government Electricity Agency

The National Electricity Agency is an agency of the Indirect Federal Public Administration that is responsible for regulating and supervising the production, transmission, distribution and marketing of electricity in Brazil. ²⁴In 2019, the agency approved a rule governing the Data and Information Governance Policy to increase the efficiency of data management, its transformation into information and to minimise operational risks.

The Policy includes measures to streamline processes, from data collection and storage to control, protection and optimisation of data assets. But it also provides an interesting approach to data governance, such as institutional competencies to acquire, control and enhance the value of the data, while information governance is the management of data in context and for the benefit of the business. The Policy creates the role of the data custodian, who is a specialist responsible for ensuring the quality and accessibility of the data used in processes.

The structure consists of the Data and Information Governance Coordinator, linked to the Superintendency of Technical Information Management. The Coordinator is responsible for guidance, training, standard setting, guidance and support for data custodians.

Figure 8: Aneel's Data and Information Governance Policy



Source: Prepared by the author.

²⁵The Agency also has a data catalogue, briefly organised as a data inventory, which is organised by metadata type: technical or operational. Basically, the database is digitised and the technical metadata is organised, then the metadata is enriched based on the operational metadata, and finally only the data is made available in a kind of marketplace. As there is also a data glossary, the user can search for terms related to the data. Access is granted to internal users in accordance with the relevant confidentiality and data protection conditions.

²⁴ <https://www2.aneel.gov.br/cedoc/prt20196197.pdf> Accessed in September 2024.

²⁵Presentation made at the 4th Meeting of the Data Governance Forum. Available at: <https://www.youtube.com/watch?v=3X-ghn398rA>



The agency's improved data governance has facilitated the creation of tools for sharing data among different agencies and government entities.²⁶ The Electricity Transmission Concession Plan Management System, developed by the Data and Information Governance Coordination, integrates the databases of the National Electricity System Operator, the Ministry of Mines and Energy, the Energy Research Company and the agency itself. Data input is carried out automatically and the system generates reports and dashboards in a synchronised and up-to-date manner.

4.2 Financial authority and currency control governance policy

The Central Bank of Brazil (BCB, in Portuguese) is an autonomous entity linked to the Ministry of Finance whose main function is to ensure a sound and competitive financial system and promote society's economic welfare. The Bank receives a large amount of information from the national financial system, its supervised institutions and other public bodies, the management of which is essential.

²⁷In 2013, the Information Governance Policy was published, which defines the roles and responsibilities related to the use and management of information through a governance structure. It also marked the creation of the Permanent Master Data Management Programme, which refers to the databases made available at a corporate and departmental level, and the Data Quality Platform Programme (Qualidatos), which automatically monitors the quality of records, as well as the Catalogue of Information with metadata. The policy was revised and updated in 2016 to take into account the Federal Government's Open Data Policy. The governance structure initially consisted of the Information Governance Committee, the board of custodians, the data custodians, the Information Governance Office and the Compliance Audit. In 2019, the Information Governance Committee was restructured and an information governance model was applied to information capturing and custodianship processes. The model includes the Governance Committee, an Information Governance Office in the IT Department to provide technical support, while the Compliance Audit oversees the obligations of the data custodians and reporting by the institutions that make up the financial system, as shown in Figure 9.

Figure 9: Central Bank data governance policy and model

²⁶

<https://www.gov.br/aneel/pt-br/assuntos/noticias/2023/sistema-desenvolvido-na-aneel-automatizara-troca-de-informacoes-entre-mme-ons-e-epe> Accessed in September 2024.

²⁷Central Bank of Brazil (2020). Communication GRC 20/2020 of 26 May 2020. Minutes of the 18th meeting of the Governance, Risk and Controls Committee. Governance, Management and Risk Committee. Available at: https://www.bcb.gov.br/content/acessoinformacao/atas_grc_docs/Ata_sessao_18_Voto_20_e_Voto_21_tarjado.pdf



Source: Adapted from the CB's information governance model, chosen as the best among central banks. News. September 2018.

Therefore, the Central Bank's Information Governance Policy has a governance model and programmes to control and monitor the quality of consolidated data.²⁸ The Central Bank's policy has become a benchmark for developing policies in other organisations and bodies: Chamber of Deputies, Ministry of Justice and Public Security, National Bank for Economic and Social Development (BNDES, in Portuguese), National Treasury Secretariat (STN, in Portuguese), Office of the Comptroller General of the Union (CGU, in Portuguese).²⁹ The Policy was also recognised as the best data custodianship initiative among central banks.

In 2022, the Policy was revised to include measures relating to data sharing and personal data protection. In terms of data sharing, a catalogue was created with a descriptive list of databases available for exchange, with the appropriate categorisation. The Governance Office and data custodians are responsible for categorising the data and ensuring that it is shared with other agencies and entities of the public administration.³⁰ The office must also support and disseminate the data sharing rules regulated by Decree 10,046 of 9 October 2019, and the LGPD.

4.3 The Government Telecommunications Agency's data governance policy

The National Telecommunications Agency (Anatel) instituted the Data Governance Policy in 2014, and updated it in 2021, with the aim of ensuring greater efficiency in data management and minimising operational risks.

Much like the Central Bank, Anatel's policy covers master data, data categories and data catalogues, and a governance structure organised around the Executive Management Commission, Data Custodianship, Information Management and Libraries, and the Permanent Data Management Forum. The governance structure is responsible for mediating technical and operational conflicts in data management, seeking data integration and optimisation, and

²⁸Central Bank of Brazil (2020). Communication GRC 20/2020 of 26 May 2020. Minutes of the 18th meeting of the Governance, Risk and Controls Committee. Governance, Management and Risk Committee. Available at: https://www.bcb.gov.br/content/acessoinformacao/atas_grc_docs/Ata_sessao_18_Voto_20_e_Voto_21_tarjado.pdf

²⁹<https://www.bcb.gov.br/detalhenoticia/291/noticia> Accessed in September 2024.

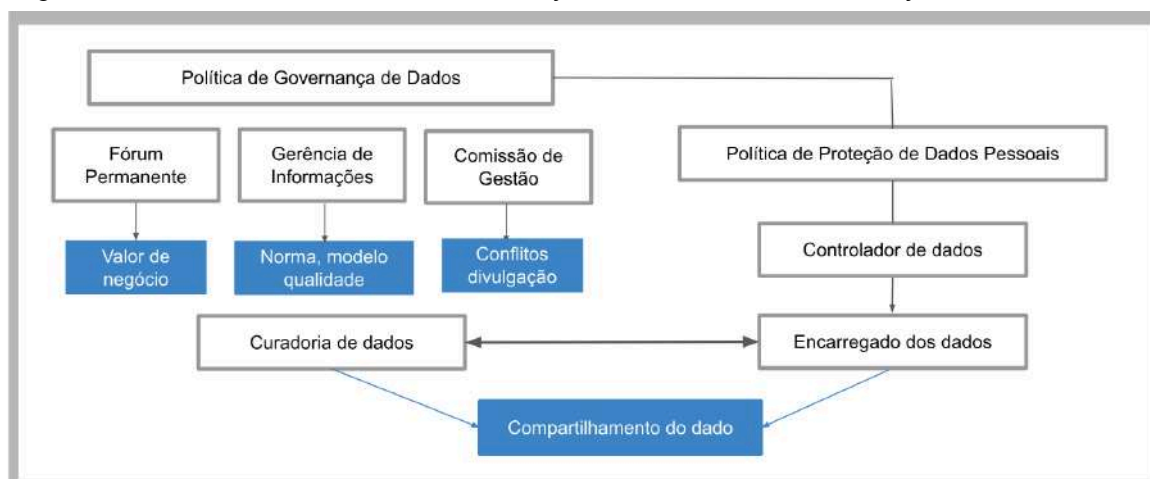
³⁰Central Bank of Brazil (2022). BCB Resolution No. 249 of 5 October 2022. Publishes the Information Governance Policy of the Central Bank of Brazil. Available at: <https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=249>



developing data collection procedures and data quality criteria. Information and Library Management is responsible for the data catalogue, the definition of standards and guidelines for data modelling and management, data quality measurement and assurance, and technical support for the other elements of the governance structure. The Permanent Forum must promote the integration of the Data Custodianships and express its views on the collection and retention of data related to the commercial interests of the agency.

³¹Data sharing is governed by the Personal Data Protection Policy of the National Telecommunications Agency, as shown in Figure 10. The policy states that data sharing must follow the terms of the legislation and be included in the Data Inventory. As a data controller, the Agency may share the data subject's personal data, subject to consent. Third-party sharing measures should be listed in the Inventory according to the classification of the data. ³²The Inventory contains a section with all the data shared with other public sector bodies and entities.

Figure 10: Anatel's Data Governance Policy and Data Protection Policy



Source: Prepared by the author.

4.4 Data and Infrastructure Policy Information Committee

The Ministry of Infrastructure, now the Ministry of Transport, instituted the Data Governance Policy in 2021, where it created the Data and Information Governance Committee. The main objective of the Committee is to improve the management, availability, quality and transparency of data and information that are essential to the Ministry's operations.

The Data and Information Governance Committee is responsible for overseeing and improving all aspects relating to the data and information generated, held or received by the ministry, such as the definition of the data cataloguing and custodianship strategy, the publication of standards and guidelines, from analysis to data sharing with other entities and agencies in accordance with current regulations.

³¹Anatel. National Telecommunications Agency (2021). Anatel Internal Resolution no. 24, of 7 June 2021. Establishes the Personal Data Protection Policy of the National Telecommunications Agency. Available at: <https://informacoes.anatel.gov.br/legislacao/component/content/article/149-resolucoes-internas/1552-resolucao-interna-24>

³²<https://www.gov.br/anatel/pt-br/acesso-a-informacao/tratamento-de-dados-pessoais/compartilhamento-de-dados>
Accessed in September 2024.



5. Challenges and recommendations³⁴

Challenges and recommendations

Despite significant progress in data governance and data sharing in Brazil, as demonstrated by success stories and capacity building initiatives, considerable challenges remain. Implementing a unified national strategy, improving coordination between different levels of government and strengthening public participation are essential for strengthening data governance and ensuring effective and transparent management. The proposed recommendations aim to address these gaps and promote a stronger and more cohesive approach to data governance in the public sector.

The analysis of data governance in Brazil highlights the following challenges and recommendations:

- **Policies and Strategies:** The country lacks a formal national framework for data governance that links the policies and strategies of states and municipalities. Coordination among different government bodies is still limited, which hampers uniform policy implementation and data sharing within the Federal Public Administration. It is hoped that with the Data Governance Policy in the federal government, this scenario will move forward and can be replicated for the other federal entities.
- **Regulation:** the regulatory framework is based on the Digital Government Law but is still developing and there are challenges in aligning data sharing, especially with the General Data Protection Act (LGPD), with the need for interoperability of public systems and the tendency for new obstacles to emerge, such as security and sovereignty of infrastructures. The legislation needs to be updated and include assumptions on public digital infrastructures, as well as conditions for its adoption by states and municipalities to reinforce the data governance recommendations of the National Digital Government Strategy.
- **Coordination and Implementation:** Coordination between federal agencies and at the local and national levels still needs to be strengthened. The implementation of data governance policies is hampered by the lack of a formal coordination structure. It is necessary to consider that a large amount of data is transmitted by national systems involving states and municipalities, and the principles of Data Cataloguing should be adopted by all public sector bodies and entities. As far as the Federal Public Administration is concerned, there are bodies and entities with consolidated governance structures and policies that should be replicated or adapted for other bodies. An investment of organisational resources is therefore essential to promote the new governance framework that will soon be in place.

³⁴Information on the Policy was obtained through interviews with members of the Central Data Governance Committee between August and September 2024. Notes were taken during the interviews. Additional content was sourced from: Central Data Governance Committee. National Data Infrastructure. Information Technology Directorate of the Shared Services Secretariat. Data Governance Week. Ministry of Public Service Management and Innovation. Available at: <https://www.youtube.com/watch?v=Fh4jgkzXuJl>



- Resources and Capacities: there is a lack of training in data governance at all levels of government. Although the governance structure has instruments in place to foster this knowledge network, the maturity of human resources and technological resources needs to be assessed and measured to ensure the effective implementation of policies, especially in the areas of interoperability and data security and in relation to the applications foreseen with the adoption of artificial intelligence in the public sector.
- Public participation: there is a need to strengthen public participation through regular public consultations, including on the Data Governance Policy, as a measure of social control, and to increase civil society's involvement in the formulation of the data governance policy.



References

- OECD. 2021. Recommendation of the Council on Enhancing Access to and Sharing of Data. Janssen, Marijn & Brous, Paul & Estevez, Elsa & Barbosa, Luis & Janowski, Tomasz (2020). Data governance: Organising data for trustworthy Artificial Intelligence. Government Information Quarterly. 37. 101493. 10.1016/j.giq.2020.101493.
- Campion, A., Gasco-Hernandez, M., Jankin Mikhaylov, S., & Esteve, M. (2022). Overcoming the Challenges of Collaboratively Adopting Artificial Intelligence in the Public Sector. Social Science Computer Review, 40(2), 462-477. <https://doi.org/10.1177/0894439320979953>
- Van Maanen, G. & Ducuing, C. & Fia, T. (2024). Data commons. Internet Policy Review, 13(2). <https://doi.org/10.14763/2024.2.1748>
- BASTOS, C. R.; MARTINS, I. G. (Org.). *Comentarios sobre la Constitución brasileña* (Comments on the Brazilian Constitution). São Paulo: Saraiva, 1989.
- EPIK, M. *Derecho a la información: situación jurídica y desafíos* (Right to information: legal situation and challenges). Informática Pública, Belo Horizonte, v. 2, n. 2, p. 43-56, 2000.
- DINIZ, V. *La historia del uso de la tecnología de la información en la gestión pública brasileña a través del CONIP – Congreso de Informática Pública* (The history of the use of information technology in Brazilian public management through the Congress of Public Information Technology). In: 10th INTERNATIONAL CONGRESS OF CLAD ON STATE AND PUBLIC ADMINISTRATION REFORM, 2005, Santiago. Annals... Chile, 2005.
- Diniz EH, Barbosa AF, Junqueira ARB, Prado O. *Gobierno electrónico en Brasil: una perspectiva histórica basada en un modelo de análisis estructurado* (e-Government in Brazil: a historical perspective based on a structured analysis model). Rev Adm Pública [Internet]. 2009 Jan;43(1):23-48. Available at: <https://doi.org/10.1590/S0034-76122009000100003>
- Brazil. Ministry of Planning, Budget and Management. Secretariat for Logistics and Information Technology. Data standard, integration of Federal Government protocols: version 2.0 / Ministry of Planning, Budget and Management. Secretariat for Logistics and Information Technology, Ministry of Justice, National Archives. – Brasília: MP/SLTI, 2015.
- <https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/catalogo-de-bases-de-dados/catalogo-de-bases-de-dados>
- Ministry of Service Management and Innovation. 2023. Data Governance Handbook. Central Data Governance Committee. Volume II. Data Ecosystem of the Federal Executive Branch. Public. Available at:



<https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadedados/arquivos/CartilhadeGovernancadeDadosEcossistemadeDados.pdf>

Ministry of Service Management and Innovation. 2023. Data Governance Handbook. Federal Executive Branch, Central Data Governance Committee. Volume II. Data Ecosystem of the Federal Executive Branch. Public. Available at: <https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadedados/arquivos/CartilhadeGovernancadeDadosEcossistemadeDados.pdf>

Ministry of Service Management and Innovation. 2023. Data Governance Booklet. Federal Executive Branch, Central Data Governance Committee. Volume II. Data Ecosystem of the Federal Executive Branch. Public. Available at: <https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadedados/arquivosCartilhadeGovernancadeDadosEcossistemadeDados.pdf>

Central Data Governance Committee. National Data Infrastructure. Information Technology Directorate of the Shared Services Secretariat. Data Governance Week 2024. Ministry of Public Service Management and Innovation. Available at: <https://www.youtube.com/watch?v=Fh4jgkzXujI>

<https://www.gov.br/gestao/pt-br/acesso-a-informacao/institucional/competencias/secretaria-de-governo-digital>

<https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/catalogo-de-bases-de-dados/catalogo-de-bases-de-dados>

Ministry of Public Service Management and Innovation. November 2023. <https://www.gov.br/governodigital/pt-br/IND/registros-de-referencia>

<https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/interoperabilidade>

Central Data Governance Committee (2024). Data Maturity. DATA MATURITY TECHNICAL GROUP. Technical Subcommittee on Data Governance. Digital Government Secretariat. Available at: <https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/maturidade-de-dados/arquivos/modelo-maturidade-de-dados-mmd.pdf>

<https://www.gov.br/governodigital/pt-br/governanca-de-dados/forum-governanca-de-dados/cartilha-de-governanca-de-dados-volume1-8-12.pdf>

<https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadedados/arquivos/CartilhadeGovernancadeDadosEcossistemadeDados.pdf>

Regarding the Forum, for presentations and access to meetings, visit: <https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadedados/forum-de-governanca-de-dados> Accessed in September 2024.



<https://www.gov.br/servicoscompartilhados/pt-br/semana-da-governanca-de-dados#:~:text=O%20evento%20acontecer%C3%A1%20entre%20os,de%202024%2C%20em%20formato%20h%C3%ADbrido.>

<https://www2.aneel.gov.br/cedoc/prt20196197.pdf> Accessed in September 2024.

Presentation made at the 4th Meeting of the Data Governance Forum. Available at:

<https://www.youtube.com/watch?v=3X-ghn398rA>

<https://www.gov.br/aneel/pt-br/assuntos/noticias/2023/sistema-desenvolvido-na-aneel-automatizara-troca-de-informacoes-entre-mme-ons-e-epe> Accessed in September 2024.

Central Bank of Brazil (2020). Communication GRC 20/2020 of 26 May 2020. Minutes of the 18th meeting of the Governance, Risk and Controls Committee. Governance, Management and Risk Committee. Available at:

https://www.bcb.gov.br/content/acessoinformacao/atas_grc_docsAta_sessao_18_Voto_20_e_Voto_21_tarjado.pdf

Central Bank of Brazil (2020). Communication GRC 20/2020 of 26 May 2020. Minutes of the 18th meeting of the Governance, Risk and Controls Committee. Governance, Management and Risk Committee. Available at:

https://www.bcb.gov.br/content/acessoinformacao/atas_grc_docsAta_sessao_18_Voto_20_e_Voto_21_tarjado.pdf

<https://www.bcb.gov.br/detalhenoticia/291/noticia> Accessed in September 2024.

Central Bank of Brazil (2022). BCB Resolution No. 249 of 5 October 2022. Publishes the Information Governance Policy of the Central Bank of Brazil. Available at:

<https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=249>

Anatel. National Telecommunications Agency (2021). Anatel Internal Resolution no. 24, of 7 June 2021. Establishes the Personal Data Protection Policy of the National Telecommunications Agency. Available at:

<https://informacoes.anatel.gov.br/legislacao/component/content/article/149-resolucoes-internas/1552-resolucao-interna-24>

<https://www.gov.br/anatel/pt-br/acesso-a-informacao/tratamento-de-dados-pessoais/compartilhamento-de-dados> Accessed in September 2024.

Brazil. Ministry of Infrastructure (2022). Data and Information Governance Coordination CODIN/MINFRA Resolution No. 5 of 1 June 2022. Available at:

https://www.gov.br/transportes/pt-br/assuntos/governanca-antigo/governanca-de-dados/normativos/sigepe_publicacao_resolucao_n_5.pdf



Annex: Legislative landscape

This section was prepared on a pro bono basis by the law firm **KLA Advogados** in Brazil, based on a connection facilitated by TrustLaw, the global legal pro bono network of the **Thomson Reuters Foundation**. Its purpose is to contextualise the legal framework applicable to data sharing, providing a legal basis that enriches the analysis of this case study.

Disclaimer of liability: This report is offered for information purposes only. It is not legal advice. Readers are urged to seek advice from qualified legal counsel in relation to their specific circumstances. We intend the report's contents to be correct and up to date at the time of publication, but we do not guarantee their accuracy or completeness, particularly as circumstances may change after publication. The Latin American Open Data Initiative (Iniciativa Latinoamericana por los Datos Abiertos, ILDA), KLA Advogados and the Thomson Reuters Foundation accept no liability or responsibility for actions taken or not taken or any losses arising from reliance on this report or any inaccuracies herein.

KLA Advogados has generously provided pro bono research to ILDA. However, the contents of this report should not be taken to reflect the views of KLA Advogados or the lawyers who contributed.

Similarly, the Thomson Reuters Foundation is proud to support our TrustLaw member ILDA with their work on this report, including the publication and the pro bono connection that made the legal research possible. However, in accordance with the Thomson Reuters Trust Principles of independence and freedom from bias, we take no position on the contents of, or views expressed in, this report.

Through a jointly developed questionnaire, KLA Advogados was asked to answer the following questions on the Brazilian regulatory framework:

1. Introduction

In Brazil, the regulatory landscape related to the use, collection and processing of data is multifaceted, encompassing laws, regulations, strategies and public policies. At the forefront of this framework is Brazil's General Data Protection Law (LGPD), Federal Law No. 13,709/2018, which establishes comprehensive guidelines for the protection and responsible use of personal data. This landmark legislation, effective as of 18 September 2020, aligns Brazil's data protection standards with international standards, marking a significant advance in the country's data privacy landscape.

Complementing the LGPD, sector-specific regulations, court rulings and agreements also play a crucial role in the implementation and evolution of data use and processing standards. Together, these elements ensure robust protection in an increasingly interconnected and data-centric world.

These guidelines elaborate on the key aspects of data protection in Brazil, focusing on the management and exchange of personal data by public bodies and agencies. They detail the regulatory framework, including the LGPD and specific guidelines for data sharing in the public sector, underlining the principles of transparency, accountability and the safeguarding of individual rights in all data processing activities.



2. What is the current legal framework, including laws, regulations, strategies and public policies, regarding the use, collection and processing of data in Brazil?

a. Brazilian regulatory landscape regarding data protection

Brazil's General Data Protection Law (LGPD), Federal Law No. 13,709/2018, establishes the fundamental guidelines for the protection and responsible use of personal data in Brazil. It represents a regulatory breakthrough, bringing Brazil's data protection legislation into line with international standards. Signed by the President on 14 August 2018, published on 15 August 2018 and effective from 18 September 2020, the LGPD marked a significant change in how personal information is treated in Brazil.

While the LGPD provides specific guidelines on the collection, use and processing of personal data, data protection and privacy rights in Brazil are also governed by a patchwork of sector-specific laws covering areas such as consumer rights, finance, health, the public sector and criminal law.

In this context, it is essential to emphasise that the Civil Internet Framework, enacted in 2014 by Law No. 12,965, together with its complementary decree, Decree No. 8,771 of 2016, established the principles, guarantees, rights and duties for the use of the internet in Brazil, including guidelines on personal data protection, net neutrality and the responsibility of intermediaries, and it established the fundamental legal framework for the online processing of personal data in Brazil. This landmark legislation not only addressed fundamental principles such as net neutrality, freedom of expression and privacy, but also established clear guidelines for the collection, storage and processing of personal data on digital platforms. In doing so, the Civil Internet Framework created a legal basis that paved the way for more comprehensive regulations, such as the LGPD, ensuring the protection of individual rights in the evolving digital landscape.

Furthermore, to further demonstrate Brazil's commitment to this scenario, in 2022, personal data protection was explicitly recognised as a fundamental right in the Brazilian Federal Constitution (Article 5, LXXIX). This inclusion underlines the high level of protection and the priority given to safeguarding personal data in the country.

b. Summary of the LGPD

The LGPD aims to protect fundamental rights, such as freedom and privacy, while promoting the personal development of individuals. It defines personal data as any information relating to an identified or identifiable individual. This includes not only details that directly identify a person, such as names and identification numbers, but also information that, when combined or analysed, can reveal an individual's identity.

The Law also introduces a definition for sensitive personal data, which is classified as any personal information relating to racial or ethnic origin, religious beliefs, political opinions, membership of trade unions or religious, philosophical or political organisations, as well as data on health, sexuality and genetic or biometric details. The processing of these categories of personal data presents significant risks to an individual's fundamental rights and freedoms, requiring a higher standard of protection under the Law.

Having set out these main definitions, it is significant to note that the LGPD applies to any personal data processing activity carried out by individuals or legal entities, whether private or public, irrespective of the method of processing (online or offline), the location of the company's



headquarters or the location of the data, provided that: (i) the processing is carried out within the national territory; (ii) the processing activity is for the purpose of offering or providing goods or services to individuals located within the national territory; (iii) the processing activities are for the purpose of processing the data of individuals located within the national territory; or (iv) where the personal data have been collected within the national territory.

It is important to note that the LGPD does not apply to data exclusively associated with legal entities. It also excludes data processing carried out by individuals solely for personal and non-commercial purposes, as well as data processed exclusively for journalistic, artistic, public security, national defence or state security purposes or for activities related to the investigation and suppression of crime. Data originating outside Brazil that is not communicated or shared with Brazilian processing agents is also outside the scope of the LGPD.

c. Brazilian National Data Protection Authority (ANPD)

The Brazilian National Data Protection Authority (ANPD), as the central authority responsible for ensuring the protection of data subjects' personal data, oversees data processing activities and provides regulatory guidance on issues requiring further clarification under the LGPD. Established as an autonomous entity linked to the Ministry of Justice and Public Security, the ANPD started its activities in November 2020.

The functions and powers of the ANPD include: (i) guaranteeing the protection of data subjects' rights, (ii) supervising and monitoring personal data processing activities carried out by public and private actors, (iii) imposing administrative sanctions in case of violations of the LGPD, (iv) guiding and educating society on rights and duties related to personal data, and (v) promoting national and international cooperation on the subject.

d. Specific guidelines for data sharing in the public sector

In the context of the public sector, Federal Decree No. 10,046/2019 establishes specific guidelines for data sharing between government agencies and entities. This decree implements the Brazilian Digital Government Strategy and facilitates data sharing within a framework of legality, transparency and security.

The decree also established the "Data Catalogue", which operates as a centralised tool for registering and sharing databases among government agencies, promoting a coordinated and efficient approach to data management. Furthermore, it stresses that any data sharing between public entities must comply with the principles of the LGPD and ensure that the rights of data subjects are protected.

To reinforce this structure, Brazil launched the Gov.br platform, which facilitates the delivery of digital public services and promotes a citizen-centred approach. This platform consolidates government information and services in a single digital environment, improving the accessibility and transparency of public data.

3. Challenges and opportunities related to data sharing in Brazil

a. Challenges

Despite regulatory advances, challenges remain in data sharing in Brazil, especially in the public sector. The key challenges include:

1. **Regulatory compliance and harmonisation:** The coexistence of multiple sector-specific laws and regulations can complicate compliance and implementation.



2. **Technical and cultural skills:** There is a need for training of public servants in data handling and processing, as well as a cultural shift towards the adoption of data sharing practices.
3. **Data infrastructure:** The lack of adequate digital infrastructure and uniform technical standards hampers data sharing between entities.
4. **Protection of sensitive data:** Ensuring the security and privacy of personal data, especially sensitive data, remains a critical challenge.

b. Opportunities

However, the regulatory framework also offers significant opportunities to make progress in data sharing:

1. **Digital innovation:** Data-centric policies can foster innovation in digital services, improving efficiency and access in key sectors such as health and education.
2. **International collaboration:** By aligning its standards with international best practices, Brazil is well positioned to participate in global data sharing initiatives.
3. **Improving public policies:** Effective use of public data can significantly improve the design, implementation and evaluation of public policies.

4. Conclusion

Brazil's regulatory framework for the use, collection and processing of data, led by the LGPD, reflects a strong commitment to personal data protection and the promotion of responsible data sharing practices. While challenges exist, the country is well positioned to take advantage of data opportunities as a strategic resource for social and economic development. Continued investment in digital infrastructure, education and data governance will be crucial to overcome barriers and unlock the full potential of a robust data ecosystem.