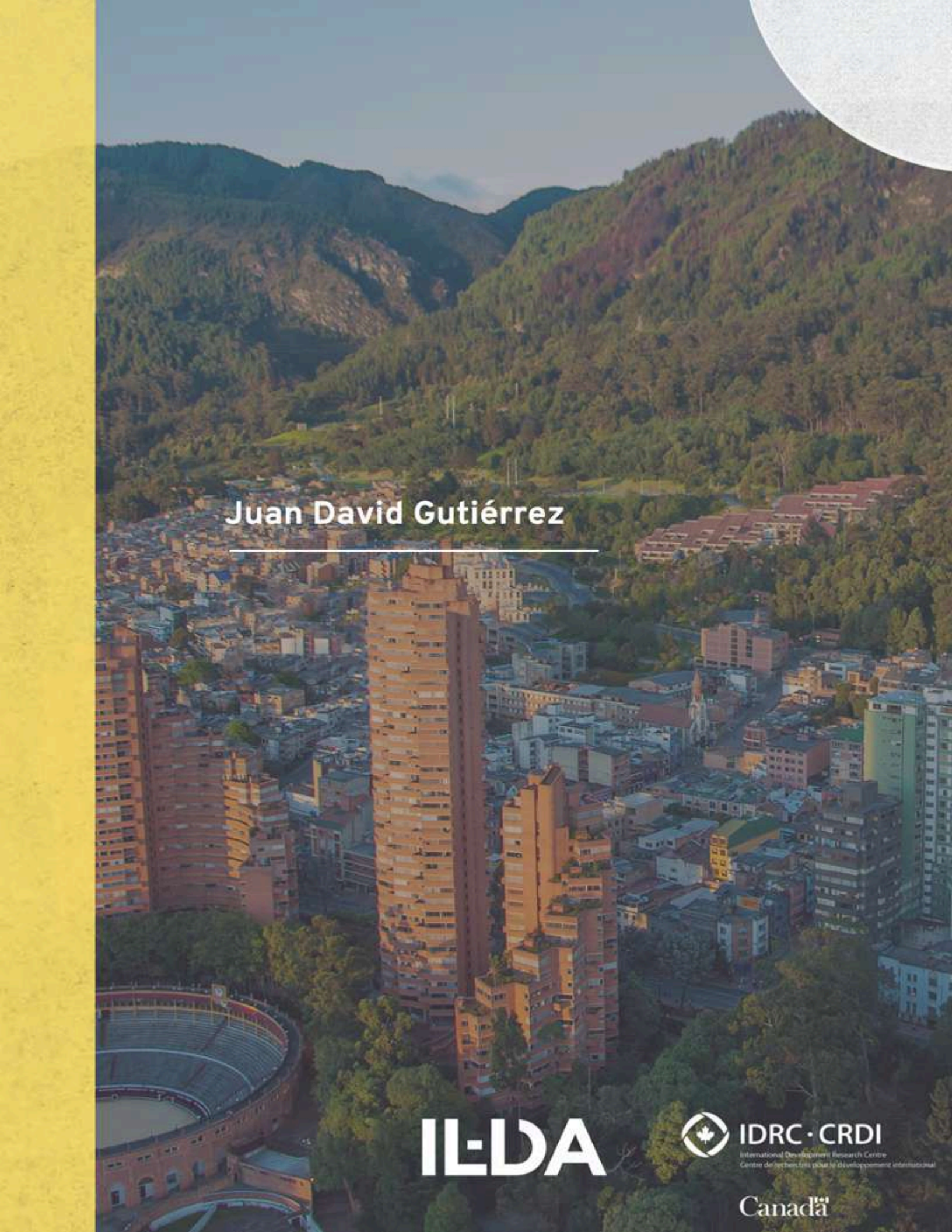




Juan David Gutiérrez

ILDA



IDRC · CRDI

International Development Research Centre
Centre d' recherches pour le développement international

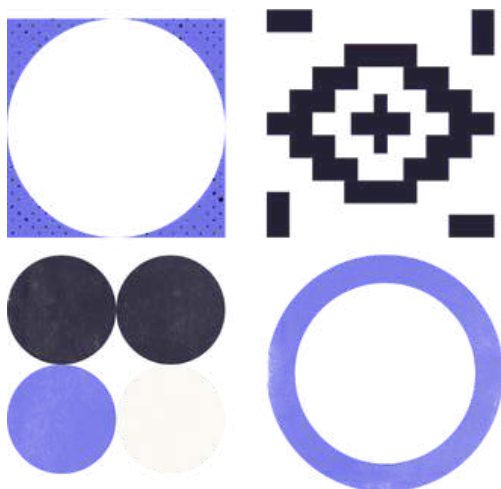
Canada



We are especially grateful to **Juan David Gutiérrez**, who carried out the research that underpins this report.

Juan David Gutiérrez is an associate professor in the School of Government at Universidad de los Andes, where he teaches and researches public policy, public management and artificial intelligence. He holds a PhD and MSc in Public Policy from Oxford University and a joint LLM in Law and Economics from the University of Bologna and Erasmus University Rotterdam. He graduated in Law from Universidad Javeriana, and he is also a member of the expert group of the Global Partnership on Artificial Intelligence (GPAI), where he leads the project on algorithmic transparency in the public sector.

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:**

Juan David Gutiérrez

PhD

Legal overview:

Dr Pablo Márquez and Dr Juan Pablo Otero from ECIJA Colombia, 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 ECIJA Colombia, the lawyers who contributed, the Patrick J. McGovern Foundation, or Thomson Reuters Foundation. Similarly, ECIJA Colombia, 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

Translation:

Supported by the Thomson Reuters Foundation, through a partnership with the Patrick J. McGovern Foundation

Acknowledgements:

International Development Research Centre (IDRC)



Index

Index	4
Foreword	5
Introduction	7
1. Background and context regarding data governance in the country	8
2. Regulatory frameworks for data protection and data sharing	15
2.1 Regulatory framework on personal data protection and privacy	15
2.2 Regulatory framework on exchange of personal data	16
2.3 Regulatory framework on data sharing between public bodies	18
3. Process of implementation of data sharing strategies and/or regulations between the relevant areas of government or externally	20
3.1 Balance of implementation: mixed results	20
3.2 Public-private partnerships	23
3.3 Technical and financial capacity and intra-state coordination	23
4. Mapas Bogotá: an example of data sharing for the generation of public value	24
4.1 Data interoperability between the State and different actors	25
4.2. Information security and personal data protection	26
4.3 Management and coordination of geographical data in Mapas Bogotá: regulations and standards	27
4.4. Generating public value through geospatial data	27
5. Challenges and opportunities	30
5.1 Five main challenges	30
5.2 Three main opportunities	31
References	33
Annex: Legislative landscape	37



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 Colombia is presented below, led by Dr Juan David Gutiérrez and the law firm ECIJA Colombia. In the case of Colombia, the document is organised into five key sections covering the context and background of data sharing governance, the characteristics of the data infrastructure and implementation processes, the regulatory framework regarding personal data protection, developments in multi-stakeholder participation in governance, and a Colombian public sector case study around the “Mapas Bogotá” initiative, which exemplifies inter-institutional collaboration through data sharing. It also presents reflections on the challenges and opportunities associated with the governance of data sharing in the country.

In terms of challenges, Colombia faces difficulties in the effective implementation of existing policies, the lack of a comprehensive regulatory framework for data sharing, the need for greater involvement of external actors in governance processes, as well as personal data protection and the improvement of interoperability between public entities. However, there are important opportunities for progress, including promoting public innovation based on data sharing, strengthening Open State policies and enhancing public–private partnerships.

This case study contributes to the formulation of strategies to consolidate a more efficient, inclusive and transparent data sharing system in Colombia, which has the potential to generate public value and strengthen democracy.



Introduction

This document presents the results of research aimed at analysing and understanding how data sharing systems work in Colombia. There are different definitions of the term “data sharing”, but in this document we will use it to mean “the process of giving third parties access to the datasets of others. These third parties may be other companies (...), private individuals or public entities” (Jussen et al., 2023, p. 3688).

The study contributes to a larger project by the Latin American Open Data Initiative (Iniciativa Latinoamericana por los Datos Abiertos, ILDA) whose final outcome will be to propose a set of good practice criteria for robust, sustainable, inclusive, and democracy- and human rights-centred data sharing frameworks.

The research was based on a review of secondary sources produced by academics and civil society organisations, an analysis of primary documentary information (regulations, procedural manuals and official reports) and information gathered from interviews with public officials, academics, experts in personal data protection and representatives of civil society.

The document was developed in five sections presenting the background and context of data sharing governance; the data infrastructure and its characteristics, processes and implementation; the regulatory frameworks on personal data protection with an emphasis on data sharing rules; the implementation of rules and strategies, as well as the participation of various actors (public, private and civil society); a case study of the Colombian public sector (“Mapas Bogotá”) that helps generate public value through multi-stakeholder data sharing; and reflections on the challenges and opportunities associated with data sharing governance.



1. Background and context regarding data governance in the country

1.1 Public policy frameworks on data governance

In recent years, the Colombian National Government has developed different tools to structure data governance in the country. The tools include various standards, policies, strategies and initiatives adopted and implemented over the last decade. In this section, we describe which tools have been adopted by the government, the actors involved and the interrelationships between these actors and the processes taking shape within the country's data governance framework.

In terms of public policies, several documents adopted by the National Council for Economic and Social Policy (CONPES, in Spanish)¹ stand out. These documents “embody the public policy decisions approved by CONPES and [...] are the result of coordinated and concerted work between different entities and institutions of the national government, in which specific actions are established to achieve the proposed objectives...” (DNP, 2021).

The main CONPES documents that form the background to public policy on data governance in Colombia are as follows:

- CONPES document 3589 of 2009, *Consolidation of a National Policy and the Colombian Spatial Data Infrastructure (ICDE, in Spanish)* examines the problem of a lack of coordination for the “production, availability, access and use of geographical information at the level of State entities” (CONPES, 2009).
- CONPES document 3920 of 2018 *National Policy on Data Exploitation (Big Data)* identified the need to design and implement a data infrastructure to maximise its economic and social value (CONPES, 2018).
- CONPES document 3975 of 2019 *National Policy for Digital Transformation and Artificial Intelligence* addresses the challenge of having a robust data infrastructure to support the implementation of AI systems, focusing on the creation of massive, interoperable and accessible databases (CONPES, 2019).
- CONPES document 4070 of 2021 on *Policy Guidelines for the Implementation of an Open State Model* set out the essential elements for fostering an Open State and established the principles and rules for the multiple actors involved in data management (CONPES, 2021a).

In addition, Article 147 of Law 1955 of 2019 established that the digital transformation projects of state entities at a national level must be carried out based on the principle of “full interoperability between public information systems”, among others. The same article states that “the exchange of information between public entities in electronic format, in the standards defined by the Ministry of ICT, is fully and permanently enabled, in real time when required, complying with personal data protection and safeguarding of information”.

¹CONPES is “the highest national planning authority and serves as an advisory body to the government on all aspects of the country's economic and social development. To achieve this, it coordinates and guides the bodies in charge of economic and social management in the government, through the study and approval of documents on the development of general policies, which are presented in session” (DNP, 2024).



Subsequently, CONPES document 4023 of 2021 *Policy for Reactivation, Upgrading Infrastructures and Sustainable and Inclusive Growth* identified the lack of an adequate governance framework for sustainable data management (CONPES, 2021b). In response, the Ministry of Information and Communications Technology (MinTIC) adopted the *National Data Infrastructure Plan* (PNID), through Resolution 460 of 2022, which establishes “the general guidelines for implementation of the Data Infrastructure in Colombia”² (MinTIC, 2022).

In addition, the “Technical Document and Roadmap” of the PNID proposes specific actions to increase data reuse, consolidate a data-driven public sector, foster spaces for data protection and sharing, and develop emerging technologies (MinTIC et al., 2021a). To this end, the initiative outlines different mechanisms for data use and sharing such as “Data Trust, Data Commons, Data Marketplace and data portals” (MinTIC, 2022).

As a result of the above, Decree 1389 of 2022 was also issued, which created the Data Infrastructure Governance Model with the objective of facilitating the coordination of actors, bodies, standards and other implementation elements for the use of data between the different government bodies: (i) *strategic level* (definition of policies and objectives); (ii) *tacit level* (planning and control); and (iii) *operational level* (implementation of activities) of the State (Congress of the Republic of Colombia, 2022)³. In addition, Decree 1501 of 2022 and Decree 523 of 2023 establish and designate the National Data Coordinator as the highest authority at the strategic level⁴.

The implementation of the PNID is complemented by other instruments, guides and guidelines, as illustrated in **Figure 1**:

²MinTIC Resolution 460 of 2022 defines “governance of the state data infrastructure” in the following terms: “the set of rules, policies, standards, roles and responsibilities to enhance the use and exploitation of the data infrastructure. Governance facilitates the coordination of actions by the public sector, private sector, academia and civil society, and generates a scenario of trust and security for the reuse of data in both the public and private sectors. Furthermore, the same resolution defines “data infrastructure” as “the set of shared, dynamic and standardised resources, provided by different actors, that enables the permanent provision of key data for its use and the generation of social, economic and/or public value” (MinTIC, 2022).

³Decree 1389 of 2022 defines the three levels of the Data Infrastructure Governance Model. The (i) *strategic level* “defines the policies, strategies and priorities for the development of the data infrastructure [...]”; the (ii) *tacit level* “draws up the plans, programmes, initiatives, projects, processes and procedures to achieve the objectives defined by the strategic level”; and the (iii) *operational level* “implements and carries out the guidelines, activities and tasks defined in the plans, initiatives, projects and procedures agreed by the tactical level” (Congress of the Republic of Colombia, 2022).

⁴Decree 1501 of 2022 “The presidential advisor for digital transformation and management and compliance of the Presidency of the Republic is designated as the National Data Coordinator”. // Decree 523 of 2023 “Through which the National Data Coordinator is appointed”.

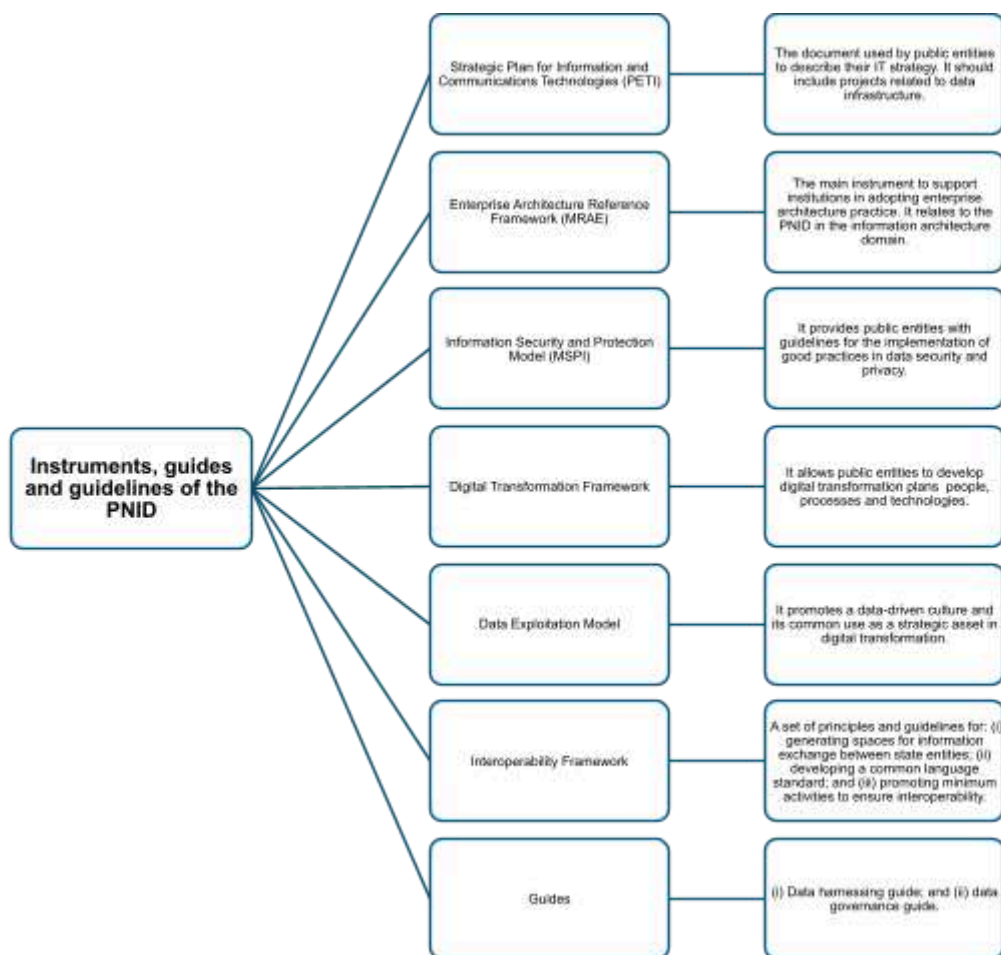


Figure 1: instruments, guidelines and guidelines of the PNID.

Source: based on the DNP (2021b).

In addition, the current national government's strategy to strengthen data governance in Colombia is organised through the National Development Plan (PND, in Spanish) 2022-2026 *Colombia Potencia de Vida*. Law 2294 of 2023, through which the PND was issued, promotes the use and exchange of data, considering interoperability as an essential "digital public asset" to guarantee human security and social justice (DNP, 2023b). Likewise, the "National Digital Strategy 2023-2026" promotes "access, use and exploitation of data to drive social transformation" (DNP, 2023a).

Similarly, the "Roadmap for the development and application of Artificial Intelligence in Colombia 2024" establishes guidelines for ethical data management in AI systems, and the draft CONPES document on *Artificial Intelligence Policy 2024* focuses on strengthening the technological infrastructure to improve the "availability, exchange and representativeness of data" in AI development (CONPES, 2024; MinTIC, 2024a).

On the other hand, by means of Law 1712 of 2014, "the Law on Transparency and the Right of Access to National Public Information is created and other provisions are



issued”. This regulation establishes the “principle of maximum disclosure”⁵, which enshrined the definition of “open data”⁶ and established general guidelines on the disclosure of public information. For the latter, the law stipulated that regulated entities⁷ must implement mechanisms and tools such as: publication schemes, active information registers, document management programmes, archives and information systems (Congress of the Republic, 2014).

Furthermore, Article 34 of the Law (amended by Law 2195 of 2022) establishes that “the design, promotion and implementation of public policy on access to public information will be the responsibility of the Transparency Secretariat of the Presidency of the Republic, which will coordinate with the Ministry of Information and Communications Technology, the Administrative Department of the Civil Service (DAFP, in Spanish), the National Planning Department (DNP, in Spanish), the General Archive of the Nation, and the National Administrative Department of Statistics (DANE, in Spanish)”.

It is worth mentioning a legislative initiative of the MinTIC that is currently being processed in the Congress of the Republic: Bill 447 of 2024 of the Chamber, “through which provisions are issued for the supply, exchange and use of the Colombian State Data Infrastructure (IDEC, in Spanish) and the interoperability of the information systems of public entities”. The text consists of 32 articles divided into four chapters on general provisions, core data infrastructure and interoperability of information systems, core data programme and interchange standards. It is aimed at both public administration entities (according to Article 39 of Law 489 of 1998) and individuals who perform administrative or public functions or administer state resources (MinTIC, 2024b). On 2 September 2024, the bill was approved in the second debate in the Chamber of Representatives (Congreso Visible Uniandes, 2024).

2.1 Participation in the construction of data governance frameworks

This section explores the different participatory spaces for the creation and establishment of data governance frameworks, examining how different actors, including government entities, civil society organisations and interest groups, contribute to the formulation of guidelines and rules governing the use and management of data.

Firstly, individuals and organisations interested in participating in legislative processes can present citizen interventions in the Congress of the Republic by virtue of Article 40 of the Political Constitution and Law 5 of 1992⁸. In the case of the main legislative proposal related to data governance, the Bill through which the MinTIC

⁵In this regard, Article 2 of Law 1712 states: “All information in the possession, control or custody of a regulated entity is public and may not be reserved or restricted except by constitutional or legal provision, in accordance with this law” (Congress of the Republic, 2014).

⁶Article 6 of Law 1712 of 2014 defines “open data” as: “all primary or raw data in standard and interoperable formats that facilitate their access and reuse, which are under the custody of public or private entities that perform public functions and which are made available to any citizen, freely and without restrictions, so that third parties can reuse them and create services derived from them” (Congress of the Republic, 2014).

⁷Article 6 of Law 1712 lists the organisations and persons to whom the law applies, including all public entities of all branches of government, independent or autonomous and control bodies, persons who perform public functions or exercise public authority, political parties and entities that administer parafiscal resources or those of public origin.

⁸Law 5 of 1992 “through which the Regulations governing the Congress, the Senate and the Chamber of Representatives are issued”. Available at <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=11368>



proposes to regulate the supply, exchange and use of the IDEC, the public was not sufficiently consulted. The Bill was not consulted on publicly and the MinTIC preferred to circulate versions of the text to a small number of universities and company representatives⁹. The Bill was only presented by the MinTIC in public discussion spaces once the legislative process had already begun.

Subsequently, during the process of admitting Bill 447 of 2024 of the Chamber, filed on 22 May 2024, only two organisations have submitted comments to date. First, the Colombian Association of Capital Cities (Asocapitales), whose main recommendation was to include a detailed description of the structure, functions and composition of the national data committee to ensure regulatory clarity, as well as aspects related to the remuneration of its members¹⁰. It also raised the need to review the fiscal impact of the Bill, as it imposes new obligations on local authorities that require additional resources¹¹. At the same time, the “data marketing ban” was questioned, suggesting an analysis of contexts in which it should be allowed¹². Similarly, it highlighted the importance of securing resources for data literacy training and the publication of the open data plan and the quality of open data in a more flexible time frame after a change of government¹³ (Asocapitales, 2024b). In response to Asocapitales’ recommendations, modifications were made to the Bill’s articles, including the approval of “amending proposals in Articles 18, 24 and 30, among others” (Asocapitales, 2024a).

Second, the firm Aledia Legaltech Colombia (ALT) submitted comments regarding the Bill, suggesting several modifications to clarify the processing of personal data¹⁴. It also stressed the need to define terms such as “anonymisation” and “pseudonymisation”¹⁵. Regarding the members of the Data Committee, it questioned “the exclusion of candidates based on specific experience, [because it could] unfairly limit opportunities for those with private sector backgrounds who could bring valuable skills and perspectives to the public sector”¹⁶. In addition, it pointed out the need to include a disciplinary regime to ensure oversight and control of the process of supply, exchange and exploitation of data s0064¹⁷ (ALT, 2024).

Secondly, administrative authorities must publish their draft regulations for comments in accordance with Article 8, paragraph 8 of Law 1437 of 2014. Subsequently, in

⁹As stated by a representative of a civil society organisation specialising in digital rights and an academic who asked to remain anonymous.

¹⁰With reference to Articles 12 and 18 of Bill 447 of 2024 of the text presented in the first debate in the Chamber.

¹¹With reference to Articles 2 and 14 of Bill 477 of 2024 of the text presented in the first debate in the Chamber.

¹²With reference to Article 19, paragraph 3 of Bill 477 of 2024 of the text presented in the first debate in the Chamber.

¹³With reference to Articles 26 and 30 of Bill 477 of 2024 of the text presented in the first debate in the Chamber.

¹⁴With reference to Article 2 (material scope related to the processing of personal data); Article 3 (definitions to include clarifications on the processing of data); Article 14 (does not establish the conditions for the processing of data subject to the law); Article 9 (on the need to implement technical and organisational security strategies in the handling of personal data) of Bill 477 of 2024 of the text presented in the first debate in the Chamber.

¹⁵With reference to Article 3 of Bill 477 of 2024 of the text presented in the first debate in the Chamber.

¹⁶Article 18 of Bill 477 of 2024 of the text presented in the first debate in the Chamber.

¹⁷With reference to Article 29 of Bill 477 of 2024 of the text presented in the first debate in the Chamber.



compliance with Decree 1081 of 2015 in Article 2.1.2.1.14.¹⁸, the administrative authorities must provide the public with a report of comments and responses to specific draft regulations. Regarding the PNID, the MinTIC published the draft of the project, during which time citizens had a period (from 15 to 17 September 2021) to make comments (MinTIC, 2021b). Subsequently, the institution published a report of observations and responses, the main findings of which were as follows: (i) there were eight submissions in total (from individuals and legal entities); (ii) a total of 49 comments were received, of which 51% were accepted and 84% were discarded; and (iii) the consultation covered 20 articles of the draft, for which 10% received comments and 50% were subject to modifications (MinTIC, 2021a).

Despite the short time allowed for comments, organisations such as the Colombian Association of Capital Cities (Asocapitales) and the Development Bank of Latin America and the Caribbean (CAF) submitted interventions. Asocapitales acknowledged the government's effort to implement a national policy focused on harnessing data. It also suggested carrying out a preliminary coordinated study with regional authorities to identify their local needs and suggestions. It also highlighted the importance of anticipating the differences that exist in terms of infrastructure and budget between capital cities in order to improve the governance and interoperability of the data infrastructure (Asocapitales, 2021). On this last point, the MinTIC welcomed the comment, highlighting that: "(i) the coordination between central and territorial levels [is] a point to be taken into account in the Governance Model"; for this purpose (ii) "the Data Exploitation Model will make it possible to guide entities in the identification of the capacities that need to be strengthened to harness the data infrastructure" (MinTIC, 2021a).

The CAF's comments were also taken into account by the MinTIC. In particular, the following points: (i) about improving the interoperability component within the framework of understanding; (ii) on the importance of including a "sectorisation" component to build specific data infrastructures in different areas (e.g. health and industry) based on practices from the European Union (EU) or Japan; and (iii) the need to seek technical cooperation to develop a Sustainability Model for Data Infrastructure (MinTIC, 2021a).

However, civil society actors such as Fundación Karisma¹⁹ criticised the excessively short deadline (15–17 September 2021) given by the MinTIC to receive comments on the draft PNID, arguing that this period was not sufficient to foster trust and effective participation of civil society as envisaged in the PNID Governance Model (Fundación Karisma, 2021). Despite the above, the organisation subsequently published its comments where it mainly questioned the lack of specific reference in the PNID to how "civil society [could] participate in the design, planning and implementation" of the project (Fundación Karisma, 2021).

The organisation also mentioned the ambiguity between the draft PNID (document) and Resolution 460 of 2022 on the Data Marketplace, as there was no "clarity about the actors interested in this market and the ways in which it will be regulated" (Fundación Karisma, 2021). It also highlighted, on the one hand, the lack of coordination of the PNID with other public policy instruments such as the National Open Data Portal and, on the

¹⁸Decree 1081 of 2015 "through which the Sole Regulatory Decree of the Presidency of the Republic Sector is issued". Available at <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=73593>

¹⁹The document with comments addressed to the PNID by Fundación Karisma was produced in partnership with Datasketch and with the support of the data governance project of the Latin American Initiative for Open Data – ILDA.



other hand, the need to mention how territorial entities could actively participate in the implementation phase of the project (Fundación Karisma, 2021).

In short, the state has opened formal spaces for participation – as provided for in the regulations – but has not worked in a participatory manner with civil society actors or academia in the construction of the different data governance instruments. However, there seems to have been a greater propensity to work with business organisations.



2. Regulatory frameworks for data protection and data sharing

2.1 Regulatory framework on personal data protection and privacy

In Colombia, the 1991 Political Constitution enshrines the fundamental rights to personal data protection and privacy (also known as the “right to *habeas data*”)²⁰. Article 15 of the 1991 Political Constitution establishes these rights in the following terms:

Article 15. All persons have the right to their personal and family privacy and to their good name, and the state must respect and enforce these rights. Similarly, they have the right to know, update and rectify the information that has been collected about them in data banks and in the files of public and private entities.

The freedom and other guarantees enshrined in the Constitution must be respected in the collection, processing and circulation of data.

Correspondence and other forms of private communication are inviolable. They may be intercepted or searched only by court order, in cases and subject to the formalities established by law.

For tax or judicial purposes and for cases of inspection, surveillance and intervention by the State, the presentation of accounting books and other private documents may be required, under the terms established by law. (Underlined excerpts are modifications outside the original text).

Since the mid-1990s, the Constitutional Court has developed a line of jurisprudence that begins to interpret the right to personal data protection as an autonomous right (with respect to the right to privacy)²¹. It is also pertinent to mention that Article 20 of the Constitution establishes the right to information and rectification, which is linked to the right to *habeas data*.

Ruling T-729 of 2002 defines the fundamental right to *habeas data* in the following terms:

It is that which grants the right to the owner of personal data to request, as a limitation on the possibilities of disclosure to the personal data administrators, access, inclusion, exclusion, correction, addition, updating and certification of the data, as well as its publication or transfer, in accordance with the principles that inform the process of administration of personal databases.

According to the Constitutional Court, five basic prerogatives grant the right to personal data protection to the owners²² of such data. These are listed below:

²⁰The Constitutional Court has also used the terms “right to digital self-determination” and “right to informational self-determination”.

²¹Rulings such as SU-082 handed down by Judge Jorge Arango Mejía in 1995 and T-176 handed down by Judge Eduardo Cifuentes Muñoz in that same year are crucial in this aspect and in the recognition that it is an autonomous right in itself.

²²Article 3 (f) of Law 1581 of 2012 defines “data subject” as an “individual whose personal data is the subject of processing”.



- i) The right to know what information there is about the data subject.
- ii) The right to update information, i.e. to update it in case of new information.
- iii) The right to rectify the information when it does not correspond to the truth, which also has to do with the right to the expiry of the data.
- iv) The right to have new data included precisely to ensure the quality of the information held in the databases.
- v) The right to exclude information that may arise from different circumstances; for example, if the data controller is misusing the information or simply due to the data subject's own wishes. Unless, of course, one of the legal exceptions applies so that, even if requested by the data subject, the data controller must maintain certain information in its databases²³.

The first statutory law that generally developed the right to personal data protection was Law 1581 of 2012²⁴. The Constitutional Court describes the model of implementation of this law as a centralised model, similar to that adopted by many European Union countries, in which a general regulation is established where all types of processing of personal data must enjoy certain minimum principles and guarantees that are common to any sector and that apply to both public and private sector individuals. Thus, there is a specialised central authority that must also be independent and autonomous and supervise compliance with the regulations²⁵: the Superintendency of Industry and Trade (SIC, in Spanish).

Law 1581 of 2012 was regulated by different decrees that were compiled by Decree 1074 of 2015 ("sole decree regulating the trade, industry and tourism sector")²⁶. In addition, the SIC has guided the implementation of the law by issuing Title V of the SIC's Sole Circular, which is particularly important, as will be explained in the next section, because it addresses the transfer of personal data to third countries.

2.2 Regulatory framework on exchange of personal data

Law 1581 of 2012 defines "database" as the "organised set of personal data that is subject to Processing"²⁷. Regarding the processing of data²⁸, the law provides that it must be carried out for a legitimate purpose in accordance with the Constitution and the law and

²³Constitutional Court, Ruling SU-082 of 1995.

²⁴Previously, Law 1266 of 2008 had regulated the processing of financial and commercial data, including personal and non-personal data, and Law 1273 of 2009 amended the Criminal Code to create new criminal offences associated with the right to *habeas data*.

²⁵Constitutional Court, Ruling C-748 of 2011.

²⁶Subsequently, the Congress of the Republic has passed laws associated with the right to *habeas data*, such as Law 2300 of 2023 ("through which measures are established to protect consumers' right to privacy").

²⁷Article 3 (b) of Law 1581 of 2012.

²⁸Article 3(g) of Law 1581 of 2012 defines "processing" as "Any operation or set of operations on personal data, such as collection, storage, use, circulation or deletion".



that the data controller²⁹ and/or the data processor³⁰ responsible for the database³¹ must inform the data subject of this purpose. In addition, the regulation indicates that it is the responsibility of the data controller to identify “each of the databases it registers in accordance with the purpose for which it was created”³².

In accordance with the provisions of Law 1581 of 2012, authorisation is understood to mean the “prior, express and informed consent of the data subject to carry out the processing of personal data”³³. The law³⁴ also establishes that such authorisation must meet the following minimum requirements:

1. The granting of authorisation by the data subject must be prior³⁵, clear, express³⁶ and informed.
2. Authorisation may be obtained by any means, but proof of its granting must be preserved for later consultation (especially as it may be requested by the SIC)³⁷.
3. At the time of requesting consent, the data subject³⁸ must be intelligibly informed about:
 - a. What personal data will be collected.
 - b. The processing to which the data will be subjected, including whether they will be transferred or transmitted.
 - c. The purpose of the processing.
 - d. The optional nature of the answer to the questions put to them when they deal with sensitive data.
 - e. Their rights as a data subject.
 - f. The identification, physical or electronic address and telephone number of the data controller.

In the case of sensitive data, in addition to the above, the data subject's authorisation must be explicit³⁹ and has special information requirements⁴⁰. The regulation seeks to ensure that when the data subject decides whether to authorise the processing of

²⁹Article 3 (e) of Law 1581 of 2012 defines “data controller” as an “Individual or legal entity, public or private, who alone or in association with others, makes decisions regarding the database and/or Processing of the data”.

³⁰Article 3 (d) of Law 1581 of 2012 defines “data processor” as an “Individual or legal entity, public or private, who alone or in association with others, carries out the Processing of personal data on behalf of the Data Controller”.

³¹Article 4 (b) of Law 1581 of 2012.

³²Article 2.2.2.26.2.5 of Decree 1074 of 2015.

³³Article 3 of Law 1581 of 2021.

³⁴Articles 6 (a and b), 9, 12 and 17 of Law 1581 of 2012, Decree 1074 of 2015 and the Sole Circular of the SIC.

³⁵Pursuant to Article 2.2.2.25.2.2. of Decree 104 of 2015, authorisation must be obtained prior to the processing of the data or at the latest at the time of collection.

³⁶The data subject's consent must be based on a positive action by the data subject, e.g. a written or oral statement or unequivocal conduct. Silence or inaction cannot be considered as authorisation. See Article 2.2.2.25.2.4 of Decree 1074 of 2015.

³⁷See paragraph of Article 12, Article 17 (b) and Article 21 (f) of Law 1581 of 2012. See Article 2.2.2.25.2.5 of Decree 1074 of 2015.

³⁸Article 12 of Law 1581 of 2012 refers to the data controller's duty to inform the data subject.

³⁹“Notwithstanding the foregoing and in order to provide a solution to this question, in the case where any processing of sensitive data is carried out, the authorisation must be explicit; that is to say, it only admits the granting of consent in written or oral form and, consequently, it is not feasible to obtain said authorisation through unequivocal conduct”. (SIC, Concept No. 17- 364624).

⁴⁰Article 2.2.2.25.2.3 of Decree 1074 of 2015.



their data, they have the necessary information regarding the purposes of the processing and the terms under which it will be carried out. In other words, the aim is for the data subject's decision to be informed and for the processing to be based on the data subject's full knowledge of what is going to happen to their data.

Furthermore, under the "principle of restricted access and circulation" established by Law 1581, personal data may only be processed "by persons authorised by the data subject" and/or by the persons provided for in Law 1581 of 2012 (e.g. a public entity that requires the data for the performance of its legal functions or by court order)⁴¹. Moreover, by virtue of the same principle, if the data controller or database administrator wishes to make the personal data collected available on the internet or other mass media, it may only do so when it ensures that access to the data "is technically controllable so as to provide restricted knowledge only to data subjects or authorised third parties"⁴².

The circulation of personal data in Colombian law is regulated on the basis of two concepts: "transmission" and "transfer" of personal data. Article 2.2.2.25.1.3 of Decree 1074 of 2015 defines the transfer and transmission of personal data in the following terms:

4. Transfer: Data transfer takes place when the Controller and/or Processor of personal data, located in Colombia, sends the information or personal data to a recipient, which in turn is a Data Controller and is located inside or outside the country.
5. Transmission: Processing of personal data that involves its communication within or outside the territory of the Republic of Colombia where the purpose of the Processing is carried out by the Data Processor on behalf of the Data Controller.

The main difference between the two is that in the transfer of data, the recipient of the data becomes the data controller (can make their own decisions about the database and its processing), whereas in the transmission of data, the recipient of the data can only process it on behalf of the sender (and cannot make their own decisions about the database)⁴³.

Taking into account the principles of purpose, freedom, transparency, proportionality and necessity for the processing of personal data contained in Law 1581 of 2012 and the statements⁴⁴ of the SIC, the premises that a national data transfer or transmission should comply with are as listed below:

1. The policies of the data controller contemplate the transfer and/or transmission of data to third parties.
2. The authorisations granted by the data subjects allow the transfer or transmission of the data to third parties.
3. The recipient of the database does not process the data for a purpose other than that initially authorised by the data subjects.

In addition, in the case of transfer, the data processor must comply with the information processing policies and with the information security and privacy conditions provided by the data controller of the personal database.

⁴¹Article 4, paragraph f) and Article 10 of Law 1581 of 2012.

⁴²Article 4, paragraph f) of Law 1581 of 2012.

⁴³Article 3 of Law 1581.

⁴⁴SIC, Concept with file number 15-121139-00001-0000.



Finally, for international data transfers, Chapter Three of Title V of the SIC's Sole Circular establishes the "standards of an adequate level of protection of the country receiving the personal information" and which countries "have an adequate level of personal data protection".

2.3 Regulatory framework on data sharing between public bodies

There is currently no comprehensive regulation of the exchange of personal or non-personal data between public bodies. As mentioned in a previous section of this report, a Bill is currently being processed in the Congress of the Republic that seeks to fill this gap: Bill 447 of 2024 of the Chamber, "Through which provisions are issued for the supply, exchange and use of the Colombian State Data Infrastructure (IDEC) and the interoperability of the information systems of public entities".

However, data sharing between public entities does not take place in a regulatory vacuum. Data sharing takes place under the protection of constitutional rules such as the following:

- Principle of accountability.
- Harmonious collaboration between public authorities.
- Right of access to public information.

In addition, the above constitutional rules are further developed by other general rules that are also applicable, such as:

- Code of Administrative and Contentious-Administrative Procedure.
- Law on transparency and the right of access to national public information.
- The rules creating relevant public entities and assigning objectives, functions and responsibilities to their units and top management.

Finally, if Bill 447 of 2024 of the Chamber is approved, it is possible that questions will be raised about its constitutionality in relation to the right to personal data protection, which will end up being resolved by the Constitutional Court. On the one hand, Carolina Botero (Botero, 2024) has argued that the Bill should have recognised that the Colombian state processes personal data through its IDEC and that it should consequently take the required measures for its protection.

In contrast, what the MinTIC representatives have stated in different academic forums and public events about the Bill is that it does not touch the fundamental core of the right to personal data protection and that its objective is to facilitate the exchange of non-personal data, as this would be anonymised by each public entity before sharing.



3. Process of implementation of data sharing strategies and/or regulations between the relevant areas of government or externally

The first two sections described a broad set of strategies and rules associated with data sharing in Colombia. This section discusses some of the issues associated with the implementation of these strategies and rules.

3.1 Balance of implementation: mixed results

The Colombian National Government has not conducted any formal assessment of the implementation process of the strategies and/or regulations on data sharing between the relevant areas of government or with external parties. The lack of systematic information on these processes makes it difficult to judge their state of implementation.

The “Data Explorer” published by the Open Government Partnership (OGP) as part of its report *Broken links: open data to promote accountability and fight corruption* (OGP, 2022) identifies that in Colombia there is a significant gap between mandatorily collected data and its publication⁴⁵.

From the interviews conducted when preparing this report, it is possible to conclude preliminarily that the balance of implementation presents mixed results:

- A representative of the private sector, an expert in technology and data protection law, stated that “although certain efforts are being made in some state entities [...] there do not seem to be as many results in terms of public strategies coordinated among different entities to satisfy multiple needs of the population, or the benefits are centralised in certain population groups. Challenges remain in the effective implementation of these strategies, especially in terms of inter-agency coordination and availability of resources.”⁴⁶
- Another data protection expert who leads a civil society organisation described their assessment of the implementation of the government’s strategy as “neutral” or “average” because “on the one hand, implementing a data sharing strategy is not easy anywhere in the world and, on the other hand, progress in Colombia has been more sector-specific, in the health, financial, energy and education sectors. There has also been regulation, particularly in telecommunications, which has promoted portability and interoperability. However, the expert also points out that there have been failures in the government’s strategy because “many things have to be coordinated, not just regulatory but also technological, to enable data sharing, and the state has not been very judicious in establishing standards for information systems... what the state has done is insufficient.”⁴⁷
- One SIC official interviewed stated that “civil servants and companies still have big cultural complexes about sharing information”⁴⁸.

⁴⁵See Asset Disclosure section in the Data Explorer available at <https://www.opengovpartnership.org/broken-links/data-explorer/country/colombia>

⁴⁶The interviewee asked to remain anonymous.

⁴⁷The interviewee asked to remain anonymous.

⁴⁸The interviewee asked to remain anonymous.



- On the other hand, a former SIC official claimed that there was a gap between what was established in the rules for sharing personal data and what was actually implemented and complied with in practice⁴⁹.
- Finally, in the interview, Professor Nelson Remolina stated that significant progress has been made in data sharing between some types of public entities (e.g. superintendencies), but progress in the public sector does not seem to be homogeneous.

In addition, based on publicly available information and interviews, it is possible to identify some key implementation milestones that show the establishment of coordination agencies and tools within the state; public consultations, training and/or awareness-raising processes within the public sector; and joint work with key international actors such as the Open Government Partnership.

- **2015:** the SIC published the booklet “Personal data protection in cloud computing services.”⁵⁰
- **2016:** the SIC published the “Guide to request the declaration of conformity on international transfers of personal data.”⁵¹
- **2019:** as part of the National Statistical System, the Data Administration Committee (CAD, in Spanish) was created by Decree 2404 of 2019 to promote “secure exchanges of databases at a microdata level, in which information from different entities is produced and integrated. The CAD also aims to ensure the implementation of an ethical framework for the proper use of data.”⁵²
- **2019:** the MinTIC published the “Guide for the use and exploitation of Open Data in Colombia”⁵³.
- **2019:** was adopted from Joint External Circular No. 04 of 2019 by the SIC and the National Agency for the Legal Defence of the State on “processing of personal data in interoperable information systems”. The Circular instructs national state bodies on how they can apply the principle of full interoperability of information systems in compliance with personal data protection rules. According to one SIC official interviewed, this Circular was a response to the reluctance of public bodies to share information with each other⁵⁴.
- **2020:** the MinTIC published the “Guide to quality standards and interoperability of open data of the Colombian government”⁵⁵.
- **2021:** the SIC published the “Guide on the processing of personal data in state entities.”⁵⁶

⁴⁹The interviewee asked to remain anonymous.

⁵⁰The Booklet is available at https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Cartilla_Proteccion_datos.pdf

⁵¹Available at https://www.sic.gov.co/sites/default/files/files/Nuestra_Entidad/Publicaciones/Guia_para_solicitar_la_declaracion_de_conformidad_sobre_las_trasferencias_internacionales_de_datos_personales.pdf

⁵²Available at: <https://www.sen.gov.co/conozca-el-sen/instancias/cad>

⁵³Available at <https://herramientas.datos.gov.co/sites/default/files/Guia%20de%20Datos%20Abiertos%20de%20Colombia.pdf>

⁵⁴The interviewee asked to remain anonymous.

⁵⁵Available at: https://herramientas.datos.gov.co/sites/default/files/2020-11/A_guia_de_estandares_final_0.pdf

⁵⁶Available at [https://www.sic.gov.co/sites/default/files/files/2021/SIC%20\(2021\)%20Gu%C3%ADa%20sobre%20el%20tratamiento%20de%20datos%20personales%20en%20las%20entidades%20estatales.pdf](https://www.sic.gov.co/sites/default/files/files/2021/SIC%20(2021)%20Gu%C3%ADa%20sobre%20el%20tratamiento%20de%20datos%20personales%20en%20las%20entidades%20estatales.pdf)



- **2022:** issuance of Decree 1297 of 2022 regulating “open finance”. The open finance processes⁵⁷ led by the Financial Superintendency have increased the circulation of data in the financial sector. These processes have been embraced by the country’s *fintech* ecosystem.
- **2022:** the inter-institutional open data workshop was jointly organised by the Mayor’s Office of Bogotá, OGP and civil society organisations⁵⁸.
- **2022:** the MinTIC published documents, studies and guidelines to carry out data sharing projects in the public sector:
 - o “Guideline – Market Study in Strategic Sectors for Data Sharing Pilot Project”⁵⁹.
 - o “Selection of a use case for a Data Sharing Pilot Project”⁶⁰.
 - o “Steps for piloting Data Trust, Data Commons and Data Marketplace data sharing projects”⁶¹.
 - o “Data Commons pilot design”⁶².
- **2023:** the first session was held of the National Data Committee, which had been created by Decree 1389 of 2022 “as an inter-institutional coordination body at the strategic level that will have the purpose of promoting the policy on data infrastructure in the country and guiding actions aimed at strengthening the governance, use, circulation and reuse of data.”⁶³
- **2023:** The V Open State Action Plan (2023-2025) was created through processes that incorporated design thinking tools and with the leadership of state entities and civil society organisations of the Open Government Alliance Colombia.
- **2024:** the Ministry of Health created the Data Governance Committee in the Health Sector through Resolution 410 of 2024 “as an advisory body that will guarantee the adequate coordination and interaction between the various departments and entities” of the health sector in relation to the fulfilment of the PNID and data governance.
- **2024:** the MinTIC offered virtual courses on digital government, including data governance and open data, which are aimed at both public servants and the general public⁶⁴.

3.2 Public–private partnerships

It is possible to identify different ways in which state and non-state organisations exchange data for the generation of public value and in what ways they promote Open State initiatives. One example of collaboration mentioned by an expert interviewed for this report is how “the existence of private adjudicators exchanging, as applicable, information with state entities such as the National Directorate of Taxes and Customs (DIAN, in

⁵⁷“*Open finance* refers to the exchange of personal information on financial transactions, not only within the banking ecosystem but also among all entities supervised by the Financial Superintendency and between these and third parties” (de la Calle, n.d.).

⁵⁸More information on the workshop is available at <https://www.ideca.gov.co/node/3224>

⁵⁹Available at https://gobiernodigital.mintic.gov.co/692/articles-238508_recurso_2.pdf

⁶⁰Available at https://gobiernodigital.mintic.gov.co/692/articles-238510_recurso_2.pdf

⁶¹Available at https://gobiernodigital.mintic.gov.co/692/articles-238512_recurso_2.pdf

⁶²Available at https://gobiernodigital.mintic.gov.co/692/articles-245714_recurso_2.pdf

⁶³Minutes of the meetings of the National Data Committee available at <https://infraestructuradatos.gov.co/798/w3-propertyvalue-916010.html>

⁶⁴More information on the courses is available at <https://gobiernodigital.mintic.gov.co/portal/Cursos-Talento-GovTech/>



Spanish) or the National State Registry, has meant that, at least for these public entities, they needed to implement contractual and internal mechanisms to carry out such information flows in a secure and reliable manner”⁶⁵.

Finally, the former superintendent delegate for personal data protection of the SIC and current professor at Universidad de los Andes stated in the interview that “academia and civil society entities have played a role as co-creators or co-organisers of some policies. They raise their concerns with the government and make proposals for improvement”. However, a leader of a civil society organisation mentioned that the level of private sector involvement varies greatly by sector and that some sectors, such as finance and health, have a high level of public–private interaction and collaboration⁶⁶.

3.3 Technical and financial capacity and intra-state coordination

With regard to the technical and financial capacity to carry out data sharing projects, the interviews conducted also reveal a mixed picture:

- A private sector representative with expertise in technology and data protection law stated that “public entities in Colombia face multiple limitations in terms of human, technical and financial resources to implement projects involving data sharing.”⁶⁷
- Another civil society expert indicated that although there is heterogeneity in the availability of resources among public entities, and that there are public entities that do allocate significant resources (such as the MinTIC), in general, “the resources are insufficient”⁶⁸. In particular, the expert drew attention to the low level of coordination between the national and territorial levels and the technological precariousness of hundreds of local authorities.
- On the other hand, a SIC official stated that tools do exist for data sharing but “the biggest obstacle is the cultural mindset of how to do it.”⁶⁹
- Finally, Professor Nelson Remolina pointed out that public entities do not tend to expressly invest in data sharing. He argued that these “entities have technical resources for their day-to-day work, but they were not acquired for data sharing”.

⁶⁵The interviewee asked to remain anonymous.

⁶⁶The interviewee asked to remain anonymous.

⁶⁷The interviewee asked to remain anonymous.

⁶⁸The interviewee asked to remain anonymous.

⁶⁹The interviewee asked to remain anonymous.



4. Mapas Bogotá: an example of data sharing for the generation of public value

Mapas Bogotá⁷⁰ is an initiative promoted by the Special Data Infrastructure for the Capital District (IDECA, in Spanish) and it was created to “access and use spatial data represented in maps on the INTERNET”. This project seeks to benefit citizens, the private sector and the district administration for data-driven decision-making (IDECA, n.d.-a). Likewise, the intention is to position this tool as a data infrastructure for “citizen control [over district projects], as it provides information about issues related to the budget of the work, the progress of the work, the type of project (...) and the date on which the data was updated” (Catastro Bogotá, 2022).

At a district level, this project is aligned with the guidelines of Agreement 130 of 2004 of Bogotá City Council, which established the IDECA⁷¹ and has been catalogued by the District Government as the official instrument for consultation and access to geo-referenced information about Bogotá⁷². The project is also framed within the guidelines of CONPES document 3585 of 2009 “Consolidation of the national policy and the Colombian spatial data infrastructure” by constituting a Geographic Information System (GIS) in coordination with the Colombian Spatial Data Infrastructure (ICDE, in Spanish)⁷³ and the Special Administrative Unit of District Land Registry (UAECD, in Spanish) “to ensure the production, interoperability and access to geospatial data” in the Capital District (CONPES, 2009).

The system works through a reference map consisting of an organised set of basic spatial data, fundamental for the planning and management of the district and “standardised in 40 levels of information whose purpose is to guarantee cartographic unification under minimum quality standards to integrate, exchange and use information in Bogotá” (UAECD, 2022). The Information System “uses REST-like geographical [web] services to query, visualise, exchange and ‘download data’ on cultural, economic and social

⁷⁰ Geographical Information System Mapas Bogotá available at <https://mapas.bogota.gov.co/>

⁷¹In 2004, Bogotá City Council established the Integrated Spatial Data Infrastructure for the Capital District (IDECA) by means of District Agreement 130 with the objective of “providing the District Administration of the central and decentralised order and that of the localities, with an instrument that allows the constant identification of the condition, mobility, dynamics, expansion, processes, projects and needs of the urban and rural areas of the city of Bogotá, D.C. in order to have sufficient geo-referenced elements that allow the District authorities to serve citizens and achieve the most accurate decision-making for the benefit of the city and its inhabitants”.

⁷²Article 1 of District Decree 203 of 2011 adopted the Reference Map “as an official consultation tool for Bogotá Capital District, defined as the organised set of basic spatial data required by most of the District Administration entities and society in general”.

⁷³ Decree 3851 of 2006 had previously defined the Colombian Data Infrastructure as an “administrative system of basic official information for public use, consisting of a standardised information architecture, suitable for the transmission, quality assurance, processing, dissemination and electronic exchange of data between generators and users”. In addition, this decree defines the ICDE’s competences as “relating to land registry, inventories of physical infrastructure, mineral, water, plant and biodiversity resources, geology, geomorphology, soils, natural hazards, climatology, land cover and use, oceanography, bathymetry, property registry, list of addresses of urban and rural buildings, connections of domestic public services, and others of the same nature”.



issues in the city” (IDECA, 2024d). Finally, the system allows the user to visualise all the information in three levels of raster images: “(i) an ortho-image; (ii) a Digital Terrain Model (DTM); and (iii) a Digital Surface Model (DSM) for Bogotá and Sumapaz” (IDECA, 2024d).

Mapas Bogotá has become a key tool for territorial administration, as it has been characterised by: (i) having the capacity to be interoperable (with government and non-government actors); (ii) seeking compliance with regulations on personal data protection; (iii) adopting internal standards and processes that follow district and national policy guidelines for geographical data management; and (iv) generating public value by improving urban planning and supporting decision making based on accessible information. Each of these four points is explained below.

4.1 Data interoperability between the State and different actors

The areas of application of interoperability between public entities, according to the Interoperability Framework for Digital Government in Colombia, work through an information exchange scheme determined by the interaction of the State at three levels: (i) Government to Citizen (G2C), (ii) Government to Business (G2B), and (iii) Government to Government (G2G) (MinTIC, 2019). In the case of Mapas Bogotá, it is possible to find these three types of interactions:

- *Government to the Citizen (G2C) and Government to Business (G2B)*. The system has a collaborative mapping component where any citizen and/or company can upload information that is not registered in the Reference Map in order to cross-reference information and identify new geographical data (Catastro Bogotá, 2022).
- *Government to Government (G2G)*. According to UAECDC Circular No. 11 of 2022, the Reference Map operates with information provided by seven district entities (see **Figure 2**) that “are responsible for the production and/or custody of the fundamental geographical objects” (UAECDC, 2022).

In addition, the Mapas Bogotá Geographical Information System operates under an Open Use Licence (CC-BY 4.0) that authorises its “use”, “sharing” and “reuse” by public entities, private organisations and the general public (IDECA, 2024d).

Figure 2 illustrates how the Mapas Bogotá information exchange operates between different public and private actors:

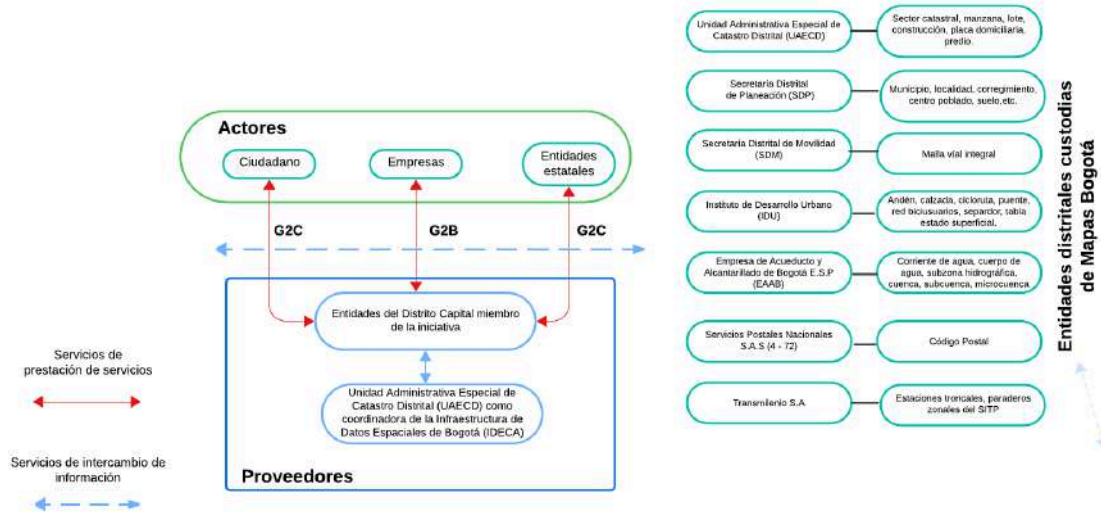


Figure 2. Information exchange services model for the Mapas Bogotá system.

Source: prepared by the author based on MinTIC, 2019; UAECDD, 2022.

4.2. Information security and personal data protection

Mapas Bogotá has 566 maps for viewing⁷⁴, of which two, to date, require the use of personal data: (i) Mapas Bogotá Bici⁷⁵, which aims to improve the experience of cyclists by providing information on route infrastructure, safety conditions and estimates related to user health (IDECA, 2023); and (ii) Agédate con Bogotá⁷⁶, which lists the events organised in the city by District entities (IDECA, 2022).

For the processing of personal data, IDECA has a “Policy on security, privacy, terms of use and personal data protection for the applications Mapas Bogotá Bici and Agédate con Bogotá”⁷⁷. The two applications listed above do not require registration, but some services do. If registration is required, users must accept the terms of use to ensure accuracy of the data and must also use the ethical and legal platforms⁷⁸. If the user does not agree to the terms of use, they may refrain from using the applications (IDECA, n.d.-b).

⁷⁴Consultation of maps available at https://www.ideca.gov.co/buscador?topic=All&metadata=All&newest=All&entity=All&resource=All&content_type=map&sort_by=created&sort_order=DESC

⁷⁵Application available at <https://www.ideca.gov.co/recursos/aplicaciones/mapas-bogota-bici>

⁷⁶Application available at <https://www.ideca.gov.co/recursos/aplicaciones/agendate-con-bogota>

⁷⁷“Policy on security, privacy, terms of use and personal data protection for the applications Mapas Bogotá Bici and Agédate con Bogotá” available at <https://www.ideca.gov.co/politicas-de-seguridad-privacidad-condiciones-de-uso-y-proteccion-de-datos-personales>

⁷⁸Specifically, the terms of use policy of the applications Mapas Bogotá Bici and Agédate con Bogotá requires consent to the following: “(a) Accept and comply with the current and applicable privacy policy. (b) Communicate changes to them in a timely manner so that they remain up to date at all times. (c) Not to use the user account for purposes or activities other than those for which it was originally created. (d) Carefully safeguard and keep the password with absolute confidentiality, preventing other persons from having access to it and immediately notifying the UAECDD of its theft and/or loss and, in general, of any improper use of the user account by third parties. (e) Not to copy or alter the pages or contents that UAECDD offers on the Internet or to link them to other Internet pages”.



In relation to the purpose for which personal data are used, IDECA's policy states that only personal data that users voluntarily provide when registering for the specific services of the applications Mapas Bogotá Bici and Agédate con Bogotá will be stored. Similarly, UAECDD must ensure "the appropriate use of the location data that the user has authorised by activating the 'background location' option" (IDECA, n.d.-b).

Additionally, at a district level, IDECA must follow the guidelines of the "Information Security and Privacy Risk Treatment Plan" and other applicable regulations of the district authorities, especially those established by the Special Administrative Unit of the District Land Registry (UAECDD) for the stipulation of the conditions of use of the applications (IDECA, n.d.-b).

4.3 Management and coordination of geographical data in Mapas Bogotá: regulations and standards

Regarding the management of the geographical data collected, Article 4, paragraph 1 of District Decree No. 203 of 2011, modified by Article 1 of District Decree No. 76 of 2013 establishes that the UAECDD "[...] as Coordinator of IDECA, and in consensus with the custodian entities, [said entity] will determine and make available through the [web] site it determines the fundamental geographical objects for the Reference Maps" (UAECDD, 2013).

Similarly, UAECDD Resolution 0454 of 2021 defines the guidelines and guiding criteria for the integrated management of data in the context of the IDEC. Mainly, it is highlighted that: (i) the UAECDD in its role as coordinator, "based on the execution of the working groups of this local initiative, will determine in agreement with the contributing entities the geographical reference data"; consequently, (ii) "these data will be socialised through circulars and the portal or website of the Official Geographical Information Platform of the Capital District or other means that are considered necessary or that replace them". Likewise, (iii) "the UAECDD [...] will continue to store the reference data provided at least quarterly by the contributing entities"⁷⁹ (UAECDD, n. d.).

In addition, Mapas Bogotá has a common language standard for information sharing whose purpose is to strengthen interoperability processes in the Capital District through the Geographical Items Registration System⁸⁰. It is a digital platform that allows the management of the complete cycle of geographical items through a dictionary of concepts and a common glossary for IDECA members (IDECA, n.d.-c). On the one hand, it allows "the creation, maintenance and publication of registers of geographical items" and, on the other hand, it assigns "unique identifiers and meanings that allow the establishment of a common language and avoid duplication of effort" (IDECA, n.d.-c).

4.4. Generating public value through geospatial data

Mapas Bogotá is a valuable tool for territorial analysis and management, as it provides essential primary data that "allows citizens to define, influence and guide their decisions and actions more easily", thus promoting greater transparency and citizen participation in public affairs (IDECA, 2024d).

⁷⁹Article 6, paragraph 1, subparagraphs (a), (b) and (c) of Resolution 0454 of 2021 of the UAECDD: "By which the guidelines and criteria for the management of the data provided in the framework of the Spatial Data Infrastructure for the Capital District (IDECA) are adopted".

⁸⁰Geographical Item Registration System available at <https://geoitems.ideca.gov.co/>



Currently, Mapas Bogotá Geographical Information System has 566 maps⁸¹ produced by the different district entities covering the following topics:

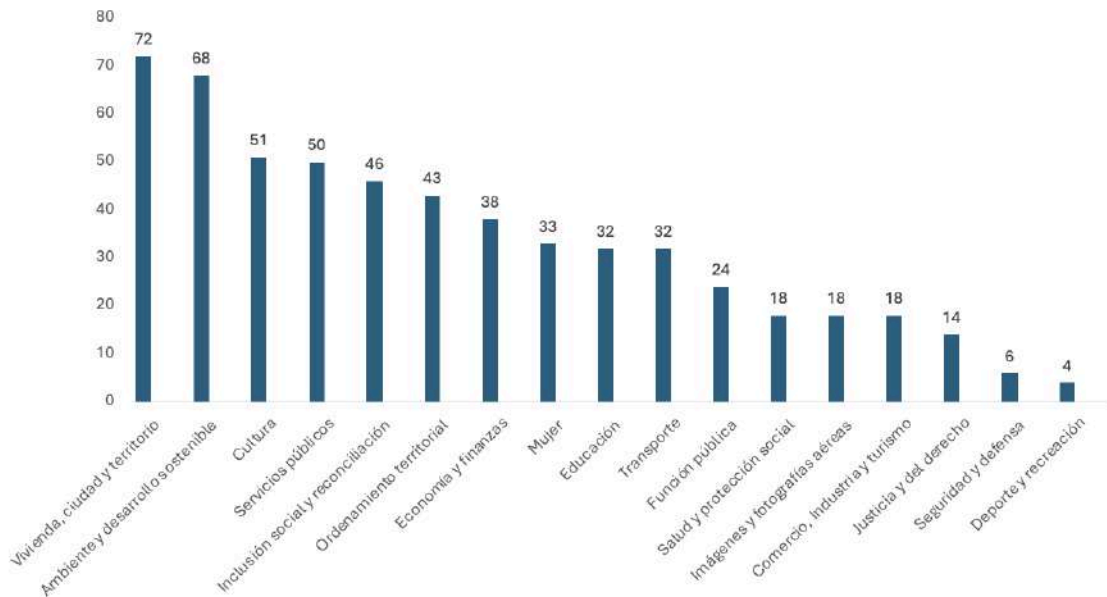


Figure 3. Different themes of maps found on the Mapas Bogotá website.

Source: prepared by the author based on IDECA, 2024b.

Among the most recent developments are: the Water Rationing Map⁸² (developed by IDECA, UAEC and the Bogotá Water and Sewerage Company) that allows citizens to “consult, through their home address, which day corresponds to their water restriction or rationing shift” (IDECA, 2024a); the Water System Map⁸³ (developed by IDECA, UAEC and the District Secretariat of Environment) that includes “all natural and artificial water bodies present in the district and the water catchment areas [...] within the framework of Decree 555 of 2021 (Land Management Plan of Bogotá D.C)” (IDECA, 2024c).

In the same way, the different entities belonging to the Capital District have built their own initiatives using the geographical data of this project as input, including the following:

⁸¹ Consultation of maps available at https://www.ideca.gov.co/buscador?topic=All&metadata=All&newest=All&entity=All&resource=All&content_type=map&sort_by=created&sort_order=DESC

⁸² Water Rationing Map available at <https://www.ideca.gov.co/node/4953>

⁸³ Water System Map available at https://mapas.bogota.gov.co/?l=63129&e=-74.4890975725308,4.476070725388313,-73.82991788503168,4.802184960498015,4.686&b=7256&show_menu=true&show_search=false



Name of the initiative	Entity in charge	Description
Arbolapp	Bogotá Botanical Garden José Celestino Mutis	Provides detailed information on the trees planted, replanted and tended in the city.
Geostatistical portal of Bogotá	District Secretariat of Planning	Provides an overview of the main Strategic City Indicators in relation to the Sustainable Development Goals (SDGs) both for Bogotá and for each locality.
Where to get vaccinated in Bogotá?	District Secretariat of Health	Web application that allows users to consult more than 300 vaccination centres.
HabitaApp	District Secretariat of Habitat	Allows monitoring of squatting and housing supply in Bogotá.

Table 1. Different initiatives of entities belonging to the Capital District in the framework of the Mapas Bogotá project.

Source: prepared by the author based on IDECA, 2024d.

In an interview with Carlos Pardo, a Colombian psychologist with a master's degree in urban planning, he highlighted both the participatory process of building the tool and its contributions to the community in terms of transforming access to information, democratising the use of geospatial data and facilitating collaboration among multiple actors. He said: "the most important thing for me is that access was made easier (and more equitable) [...]. In 2015 or later, we did a hackathon in which the first step was to help the Land Registry put data from various entities in there. It was extremely difficult, but we achieved health, security and mobility."⁸⁴

In summary, Mapas Bogotá has established itself as a strategic tool for territorial management in the Capital District thanks to its interoperability capacity, adherence to regulations on personal data protection, monitoring of internal standards to ensure the quality of geographical data and its role in the generation of public value. It represents a step forward in the district's data infrastructure, offering an open and accessible resource for citizens, businesses and authorities to optimise territorial management and strengthen citizen control.

⁸⁴Personal communication with Carlos Pardo, Colombian psychologist with a master's degree in urban planning from the London School of Economics. He has led and participated in urban development, mobility and technology projects in more than 30 cities in Asia, Latin America, Africa and the United States.



5. Challenges and opportunities

This report has highlighted that in Colombia, the governance of data sharing faces at least five main challenges and three opportunities, which are described below.

5.1 Five main challenges

Challenge 1. Implementation of existing policies. As detailed in sections 1 and 2 of this report, Colombia has a comprehensive set of strategies and policies on data sharing. However, the research indicates that there are significant gaps in their implementation. Closing the gaps requires addressing specific challenges, which include the following:

- Effective coordination between national and territorial entities and generating minimum consensus between entities on what information will be exchanged. In this regard, Professor Remolina stated that “the main challenge is to work as a team in the State and not as uncoordinated players who all want a leading role”.
- Financial investment in technical and human resources, particularly at a territorial level, so that public entities can take advantage of the State’s data infrastructure.
- Strengthening the technological infrastructure for data sharing between public entities, which, according to a civil society expert interviewed, includes reducing technological heterogeneity between public entities, e.g. information systems and communication protocols.
- Finally, the importance of maintaining policy implementation after changes of government, as Professor Remolina also highlighted in his interview.

Challenge 2. Having a comprehensive regulatory framework for data sharing. Although Colombia has some regulations on data sharing, they are scattered and have gaps. It is therefore necessary to move forward in the discussion on a regulatory framework that respects fundamental rights and facilitates coordination among public entities. This includes a broader discussion of the implications for the right to *habeas data* of Bill 447 of 2024 [“through which provisions are issued for the supply, exchange and use of the Colombian State Data Infrastructure (IDEC) and the interoperability of the information systems of public entities”].

Challenge 3. Effective participation of external actors in the governance of data sharing. Engaging civil society and the private sector in the implementation of open data strategies is crucial. However, a lack of knowledge and access to technologies can limit the effective participation of non-state actors. In addition to technology, it is necessary to build trust between citizens, civil society organisations and public entities.

Challenge 4. Personal data protection and privacy. The misuse of data (particularly personal data) can erode public trust. It is therefore important for the State to ensure that it:

- Strengthens technical, human and administrative measures for the effective protection of the right to *habeas data* by public entities. In this regard, a former SIC official interviewed argued that the oversight model of public entities is deficient because the entity in charge of ensuring compliance with data protection



regulations, the Office of the Attorney General of the Nation, in practice has not fulfilled its investigative and sanctioning role⁸⁵.

- Strengthens the capacity of public entities to comply with information security standards, especially if personal data are processed.
- Fosters a data culture through training and education to develop good practices in the processing of personal data.

Challenge 5. Interoperability and data sharing culture. The Interoperability Framework for Digital Government in Colombia emphasises the need to strengthen interoperability⁸⁶ in the public sector, so that citizens and businesses can interact with the State to acquire rights, fulfil obligations or carry out specific procedures without generating additional costs (MinTIC, 2019). To this end, one civil society expert consulted stated that the State needs to continue to work on closing technological gaps, as many public entities “have legacy systems and it is difficult to make them compatible with other modern technologies.”⁸⁷ In addition, a SIC official stated that beyond the regulatory or technological challenges, the challenge is a cultural one: “public bodies are reluctant to share the information they store” and “the biggest problem is still an issue of culture and there is a false belief in the right to *habeas data* that prohibits circulation”⁸⁸.

5.2 Three main opportunities

Opportunity 1. Promoting public innovation supported by data sharing. Access to open data can foster innovation and the development of new products and services that benefit society. In the words of an SIC official interviewed: “identifying where that exchange can generate efficiency for the provision of services, decreasing costs in economic transactions by having more and better information.”⁸⁹ Promoting public innovation initiatives that rely on data sharing involves raising public officials’ awareness of the opportunity to generate public value from more and better data that can be accessed through data sharing processes and interoperability of information systems.

Opportunity 2. Progressing and strengthening Open State initiatives. The implementation of open data policies can improve transparency and accountability in public management, strengthening democracy. To this end, facilitating access to public data can empower citizens and promote more active participation in decision-making.

Opportunity 3. Public–private co-creation and cooperation. Foster collaboration between public, private and civil society entities to create a more robust and efficient data ecosystem. In this regard, one civil society expert interviewed highlighted the importance of collaborative projects among public entities and public–private cooperation to jointly explore the types of data that could be exchanged to generate public value and avoid reprocessing of data by different entities and organisations⁹⁰. Furthermore, given that progress in such partnerships has been sector-specific, it is important to draw lessons

⁸⁵The interviewee asked to remain anonymous.

⁸⁶Interoperability is defined as the “ability of organisations to exchange information and knowledge within their business processes to interact [between citizens, businesses and other state entities] to achieve mutually beneficial goals” (MinTIC, 2019).

⁸⁷The interviewee asked to remain anonymous.

⁸⁸The interviewee asked to remain anonymous.

⁸⁹The interviewee asked to remain anonymous.

⁹⁰The interviewee asked to remain anonymous.



from the experiences of sectors that have made progress in implementing data sharing projects, such as the financial, health and education sectors.

In summary, while Colombia faces significant challenges in the governance of data sharing, there are also numerous opportunities to move towards a more transparent, inclusive and sustainable model.



References

- ALT. (2024). *Observations on Ordinary Bill 447 of 2024C of the Chamber of Representatives. "Through which provisions are issued for the supply, exchange and use of the Colombian State Data Infrastructure (IDEC) and the interoperability of the information systems of public entities and other provisions are issued"*. Available at: <https://www.camara.gov.co/sites/default/files/2024-09/Observaciones%20-%20PL%20447%20de%202024%20-%20IDEC.pdf>
- Asocapitales. (2024a). *Colombian state data infrastructure project approved in second debate*. Available at: <https://www.asocapitales.co/2024/09/aprobado-en-segundo-debate-el-proyecto-de-infraestructura-de-datos-del-estado-colombiano/>
- Asocapitales. (2024b). *Comments on Bill 447 of 2024. "Through which provisions are issued for the supply, exchange and use of the Colombian State Data Infrastructure (IDEC) and the interoperability of the information systems of public entities and other provisions are issued"*. Available at: <https://www.camara.gov.co/sites/default/files/2024-08/ASO-D-1431.pdf>
- Asocapitales. (2021). *Asocapitales' comments on the National Data Infrastructure Plan*. Available at: https://www.asocapitales.co/wp-content/uploads/2022/03/Plan-Nacional-de-Infraestructura-de-Datos_17sept2021.pdf
- Botero, C. (2024, June). MinTIC and DNP: data protection should be included for IDEC. *El Espectador*.
- Bogotá Land Registry (director). (2022, 5 October). *What you didn't know about Mapas Bogotá* [Video recording]. Available at: <https://www.youtube.com/watch?v=fITkLyYsL1M>
- Congress of the Republic of Colombia. (2022). *Decree 1389 of 2022. "Through which Title 24 is added to Part 2 of Book 2 of the Sole Decree 1078 of 2015, Regulatory Decree on the Information and Communications Technology Sector, in order to establish general guidelines for data infrastructure governance and create the Data Infrastructure Governance Model"*. Available at: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=191409>
- Congress of the Republic of Colombia. (2014). *Law 1712 of 2014. "Through which the Law on Transparency and the Right of Access to National Public Information is created and other provisions are issued"*. Available at: <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=56882>
- Visible Congress Uniandes. (2024). *General information on Project 447/24. Universidad de los Andes*. Available at: <https://congresovisible.uniandes.edu.co/proyectos-de-ley/ppor-medio-de-la-cual-se-dictan-disposiciones-para-el-suministro-intercambio-y-aprovechamiento-de-la-infraestructura-de-datos-del-estado-colombiano-idec-y-la-interoperabilidad-de-los-sistemas-de-informacion-de-las-entidades-publicas-y-se-dictan-otras-disposiciones-infraestructura-e-interoperabilidad-de-datos-del-estado-colombiano-idec/13628/>
- CONPES. (2009). *Consolidation of the national policy and the Colombian spatial data infrastructure (CONPES document 3585)*. National Council for Economic and Social Policy (CONPES). Available at:



- <https://colaboracion.dnp.gov.co/CDT/CONPES/Econ%C3%B3micos/3585.pdf>
- CONPES. De la Calle, J. M. (n. d.). *Open banking, open finance and open data*. Legal field. Retrieved on 22 September 2024, from <https://www.ambitojuridico.com/noticias/columnista-impreso/open-banking-open-finance-y-open-data>
 - CONPES. (2021a). *Policy Guidelines for the Implementation of an Open State Model (CONPES document 4070)*. National Council for Economic and Social Policy (CONPES). Available at: <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4070.pdf>
 - CONPES. (2018). *National Policy on Data Exploitation (Big Data) (CONPES document 3920 of 2018)*. National Council for Economic and Social Policy (CONPES). Available at: <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3920.pdf>
 - CONPES. (2024). *Artificial Intelligence Policy (Draft CONPES document 2024)*. National Council for Economic and Social Policy
 - CONPES. (2021b). *Policy for Reactivation, Upgrading Infrastructures and Sustainable and Inclusive Growth: New Commitment for the Future of Colombia (CONPES 4023)*. National Council for Economic and Social Policy (CONPES). Available at: <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/4023.pdf>
 - CONPES. (2019). *National Policy for Digital Transformation and Artificial Intelligence (CONPES 3975 of 2019)*. National Council for Economic and Social Policy (CONPES). Available at: <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3975.pdf>
 - DNP. (2024, 14 June). *About CONPES*. National Planning Department (DNP). Available at: <https://www.dnp.gov.co/conpes>
 - DNP. (2023a). *National Digital Strategy 2023-2026*. https://colaboracion.dnp.gov.co/CDT/Desarrollo%20Digital/EVENTOS/END_Colombia_2023_2026.pdf
 - DNP. (2021). *Methodological Manual for the creation of CONPES documents*. National Planning Department (DNP). Available at: <https://colaboracion.dnp.gov.co/CDT/DNP/SIG/M-CA06%20Manual%20metodol%C3%B3gico%20elaboraci%C3%B3n%20Doc%20Conpes.pdf>
 - DNP. (2023b). *National Development Plan (PND) 2022-2026 "Colombia, World Power of Life"*. Available at: <https://www.dnp.gov.co/plan-nacional-desarrollo/pnd-2022-2026>
 - Fundación Karisma. (2021, 16 December). *The PNID: from government to data governance?* Fundación Karisma. Available at: <https://web.karisma.org.co/el-pnid-del-gobierno-a-la-gobernanza-de-datos/>
 - IDECA. (2022 4 August). *Agéndate con Bogotá*. Ideca. Available at: <https://ideca.gov.co>
 - IDECA. (2024a). *Check your water rationing schedule*. Ideca. Available at: <https://ideca.gov.co>
 - IDECA. (2024d, 30 June). *Spatial Data Infrastructure of Bogotá*. Ideca. Available at: <https://ideca.gov.co>
 - IDECA. (2024b). *Spatial Data Infrastructure of Bogotá – Maps Section*. Ideca. Available at: <https://ideca.gov.co>
 - IDECA. (n.d.-a). *Instructions for Mapas Bogotá*. Available at: https://www.ipes.gov.co/images/informes/transparencia/Instructivo_mapas_bogota.pdf



- IDECA. (2023, 4 December). *Mapas Bogotá Bici*. Ideca. Available at: <https://ideca.gov.co>
- IDECA. (n.d.-b). *Policy on security, privacy, terms of use and personal data protection for the applications Bogotá Mapas Bici and Agédate con Bogotá*. IDECA. Retrieved on 16 September 2024, from <https://ideca.gov.co>
- IDECA. (n.d.-c). *Geographical Item Registration System*. Retrieved on 15 September 2024, from <http://geoitems.ideca.gov.co/jsp/inicio.jsp?>
- IDECA. (2024c, 19 January). *Mapas Bogotá Water System*. Ideca. Available at: <https://ideca.gov.co>
- Jussen, I., Schweihoff, J., Dahms, V., Möller, F., & Otto, B. (2023, January 3). *Data Sharing Fundamentals: Definition and Characteristics*. 56th International Conference on System Sciences. Available at: <https://hdl.handle.net/10125/103083>
- MinTIC, DAPRE & DNP. (2021b). *National Data Infrastructure Plan (Annex 1.3 Guides, instruments and guidelines)*. Available at: https://mintic.gov.co/portal/715/articles-198952_anexo_1_3_guias_instrumentos_lineamientos.pdf
- MinTIC, DAPRE & DNP. (2021a). *National Data Infrastructure Plan (Annex 1. PNID – Technical document and roadmap)*. Available at: https://mintic.gov.co/portal/715/articles-198952_anexo_1_pnid_documento_tecnico_hoja_ruta.pdf
- MinTIC. (2024a). *Roadmap for the Development and Application of Artificial Intelligence*. Available at: <https://inteligenciaartificial.minciencias.gov.co/wp-content/uploads/2024/02/Hoja-de-Ruta-Adopcion-Etica-y-Sostenible-de-Inteligencia-Artificial-Colombia-1.pdf>
- MinTIC. (2021a). *Report of observations and responses*. Available at: <https://mintic.gov.co/portal/inicio/Sala-de-prensa/179710:MinTIC-publica-para-comentarios-borrador-del-Plan-Nacional-de-Infraestructura-de-Datos>
- MinTIC. (2019). *Interoperability Framework for Digital Government*. Available at: https://lenguaje.mintic.gov.co/sites/default/files/archivos/marco_de_interoperabilidad_para_gobierno_digital.pdf
- MinTIC. (2022, 17 February). *MinTIC issues the National Data Infrastructure Plan that will drive the digital transformation of the State*. MinTIC Colombia. Available at: <https://www.mintic.gov.co/portal/715/w3-article-198952.html>
- MinTIC. (2021b). *MinTIC publishes the draft National Data Infrastructure Plan for comments*. MinTIC Colombia. Available at: <https://www.mintic.gov.co/portal/715/w3-article-179710.html>
- MinTIC. (2024b). *Bill 447 of 2024. "Through which provisions are issued for the supply, exchange and use of the Colombian State Data Infrastructure (IDEC) and the interoperability of the information systems of public entities and other provisions are issued"*. Available at: https://www.camara.gov.co/sites/default/files/2024-05/PL.447-2024C%20%28INFRAESTRUCTURA%20DE%20DATOS%20DEL%20ESTADO%20COLOMBIANO%29_0.pdf
- MinTIC. (2022). *Resolution 460. "Through which the National Data Infrastructure Plan and its roadmap in the development of the Digital Government Policy are issued, and the general guidelines for its implementation are established."* Available at: https://www.mintic.gov.co/portal/715/articles-198952_resolucion_00460_2022.pdf
- OGP. (2022). *Broken Links: Open Data to Advance Accountability and Combat Corruption*. Open Government Partnership – OGP. Available at:



https://www.opengovpartnership.org/wp-content/uploads/2023/01/OGP_BrokenLinks_FULL_single.pdf

- UAECD. (2022). *Circular No 11 of 7 December 2022 "Socialisation of the geographical information that makes up the Reference Map"*. Available at: https://www.ideca.gov.co/sites/default/files/RegistroDistrital7594_Circular11_2022.pdf
- UAECD. (2013). *District Decree No.76 of 2014 "Through which District Decree 203 of 17 May 2011 is amended"*. Available at: <https://www.catastro bogota.gov.co/normatividad/decreto-76-de-2013>
- UAECD. (n.d.). Resolution 454 of 2021. *"Through which the guidelines and criteria for the management of the data provided in the framework of the Spatial Data Infrastructure for the Capital District (IDECA) are adopted"*. Special Administrative Unit of District Land Registry – UAECD. Available at: <https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=113761>



Annex: Legislative landscape

This section was prepared on a pro bono basis by the law firm **ECIJA Colombia**, based on the 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), ECIJA Colombia 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.

ECIJA Colombia has generously provided pro bono research to ILDA. However, the contents of this report should not be taken to reflect the views of ECIJA Colombia 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, ECIJA Colombia was asked to answer the following questions on the Colombian regulatory framework.

- 1- **What is the current legal framework, including laws, regulations, strategies and public policies, around the use, collection and processing of data in Colombia?**

Data protection regulatory framework

- **Political constitution⁹¹**

Article 15 of the 1991 Political Constitution of Colombia enshrines the fundamental right of individuals to Habeas Data. In this way, it establishes that all people have the right to know, update and rectify the information that has

⁹¹Political Constitution of Colombia. 1991. Available at: http://www.secretariassenado.gov.co/senado/basedoc/constitucion_politica_1991.html



been collected about them in data banks and in the files of public and private entities.

It is on the basis of this constitutional enshrinement that the entire legal and regulatory framework for the protection and processing of personal data is developed.

- **Law 1266 of 2008**⁹²

In 2008, the Colombian Congress passed Law 1266, which develops the right to *habeas data* enshrined in Article 15 of the Constitution. In this way, the law regulates the handling of information contained in personal databases, especially financial, credit, commercial, service and third-country information.

This is a special law governing the processing of personal data of a financial nature.

Law 1266 was amended by **Law 2157 of 2021**⁹³, known as the “clean slate” law, which aims to strengthen the right to *habeas data* and establish a special regime for the handling of information associated with persons who were negatively reported in financial databases when in fact they had met their obligations. It therefore established measures related to the permanence of information in such databases, communications to data subjects and obligations on data controllers associated, for example, with the principle of accountability.

Law 1266 was regulated by **Decree 1727 of 2009**⁹⁴, which establishes the conditions under which operators of financial, credit, commercial, service and third-country information databases must submit information to data subjects. Similarly, **Decree 2952 of 2010**⁹⁵ regulated the law with regard to the special requirements for information sources and the permanence of information in databases.

The Superintendency of Industry and Commerce, in its capacity as the national authority for personal data protection, is responsible for monitoring and controlling compliance with the provisions of this law.

⁹²Congress of the Republic of Colombia. 2008. Law 1266 of 2008. Available at: http://www.secretariassenado.gov.co/senado/basedoc/ley_1266_2008.html

⁹³Congress of the Republic of Colombia. 2021. Law 2157 of 2021. Available at: http://www.secretariassenado.gov.co/senado/basedoc/ley_2157_2021.html

⁹⁴Ministry of Finance and Public Credit, Ministry of Commerce, Industry and Tourism. 2009. Decree 1727 of 2009. Available at: <https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1338429>

⁹⁵Ministry of Finance and Public Credit, Ministry of Commerce, Industry and Tourism. 2010. Decree 2952 of 2010. Available at: <https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1503907>



- **Law 1581 of 2012**⁹⁶

The next regulatory development of the provisions of Article 15 of the Political Constitution was the issuance of Law 1581 of 2012, which constitutes the current general legal framework on personal data protection.

This standard includes key provisions such as the requirement of prior, express, informed consent of the data subject for the collection and processing of their data. It defines the duties of data controllers and processors, recognises the right to deletion and restriction of use of data, and protects sensitive data in particular, allowing processing only in limited circumstances. In addition, it enshrines the principle of restricted access and circulation, stating that only authorised persons may handle the information.

It prohibits the transfer of data to countries without adequate protection, except for specific exceptions, and assigns control to the Superintendence of Industry and Commerce through its Delegation for Personal Data Protection.

2013⁹⁷, made under Law 1581, to regulate ~~the~~ the accountability principle in relation to the processing of personal data.

- Sole Circular of the SIC

The Superintendency of Industry and Commerce as the national authority on personal data included in its Sole Circular – an instrument that brings together all the regulations and general instructions of the Superintendency – a title on personal data protection. It establishes instructions related to the right of *habeas data* for financial, credit, commercial, service and third-country information, on the national registry of databases and on the transfer of personal data to third countries.

Information security

- Public Policy Document – CONPES 3854 of 2016⁹⁸

Public policy document CONPES 3854 of 2016 establishes the National Digital Security Policy. This document seeks to complement the existing cyber security

⁹⁶ Congress of the Republic of Colombia. 2012. Law 1581 of 2012. Available at: http://www.secretariassenado.gov.co/senado/basedoc/ley_1581_2012.html

⁹⁷ Ministry of Commerce, Industry and Tourism, Ministry of Information and Communications Technologies. 2013. Decree 1377 of 2013. Available at: <https://www.suin-juriscol.gov.co/viewDocument.asp?id=1276081>

⁹⁸ National Council for Economic and Social Policy – National Planning Department. 2016. CONPES 3854 of 2016. Available at: <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf>



and cyber defence policy by including risk management as a key element in addressing digital security.

In this regard, the policy has five key elements, including the creation of a clear institutional framework, the promotion of trust in the digital environment, the strengthening of digital defence at a national and transnational level, and cooperation on digital security at a national and international level.

- Public Policy Document – CONPES 3995 of 2020⁹⁹

Public policy document CONPES 3854 of 2016 establishes the National Policy on Digital Trust and Security. The policy aims to improve digital trust and security in Colombia, in order to increase the country's inclusion and competitiveness. The policy focuses on three pillars: strengthening the digital security capacities of the public, private and citizen sectors; updating the governance framework in this area; and adopting digital security models and standards with an emphasis on new technologies.

- Resolution 500 of 2021¹⁰⁰

Resolution 500 of 2021 establishes the guidelines and standards for the digital security strategy. In addition, it establishes a security and privacy model that serves as an enabler of the Digital Government policy. Thus, an Information Security and Privacy Model, an information security risk management guide and the procedure for managing digital security incidents are established, as well as guidelines and standards for the digital security strategy.

These rules are aimed at the entities that make up the public administration and individuals performing administrative functions and are therefore not a generally applicable regulation. By virtue of this Resolution, the regulated entities must apply the models, guides and technical documents established for the implementation of the information security and digital security management system. Similarly, they are obliged to adopt a digital security strategy that includes the principles, policies, procedures, guides, manuals, formats and guidelines for managing digital information security.

This resolution was subsequently supplemented by **Resolution 746 of 2022**¹⁰¹, establishing measures arising from the growing use of cloud services that

⁹⁹ National Council for Economic and Social Policy – National Planning Department. 2020. CONPES 3995 of 2020. Available at: <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3995.pdf>

¹⁰⁰ Ministry of Information and Communications Technologies. 2021. Resolution 500 of 2021. Available at: <https://www.suin-juriscol.gov.co/viewDocument.asp?id=30044822>

¹⁰¹ Ministry of Information and Communications Technologies. 2022. Resolution 746 of 2022. Available at: https://www.mintic.gov.co/portal/715/articles-208143_recurso_1.pdf



increase security risks in the processing of personal data and require greater cooperation between public entities and providers. It thus complements Resolution 500 by establishing measures for public entities and their providers to jointly manage information security risks, assessing and mitigating the impacts of changes in the supply of products or services.

- Decree 338 of 2022¹⁰²

Decree 338 of 2022 establishes general guidelines for strengthening digital security governance, identifying critical cyber infrastructures and essential services, as well as risk management and response to digital security incidents.

In this regard, the entities that make up the public administrations and individuals who perform public or administrative functions are obliged, by virtue of this decree, to adopt a digital security governance model. The law also provides for the national government, through the Ministry of Information and Communications Technologies, to draw up an inventory of critical national public cyber infrastructures and essential services in cyberspace.

- Decree 767 of 2022¹⁰³

Decree 767 of 2022 establishes the general guidelines for Digital Government. This is within the framework of the different decrees and resolutions issued (cited where relevant in this document) to integrate digital citizen services, the use of open data and the digitisation of procedures. In this context, the purpose of Decree 767 is to update the Digital Government Policy to reflect technological developments and improve service delivery through the collaboration of multiple actors and institutions.

Among the elements of the Policy, it should be noted that the regulated entities must develop, among other things, capacities through the implementation of information security and privacy guidelines in all their processes, procedures, services, information systems, infrastructure and, in general, in all information assets to preserve the confidentiality, integrity, availability and privacy of data.

Data infrastructure

- Decree 1389 of 2022¹⁰⁴

¹⁰² Ministry of Information and Communications Technologies. 2022. Decree 338 of 2022. Available at: <https://www.suin-juriscol.gov.co/viewDocument.asp?id=30043957>

¹⁰³ Ministry of Information and Communications Technologies. 2022. Decree 767 of 2022. Available at: <https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/30044202>

¹⁰⁴ Ministry of Information and Communications Technologies. 2022. Decree 1389 of 2022. Available at: <https://www.suin-juriscol.gov.co/viewDocument.asp?id=30044499>



Decree 1389 of 2022 establishes the guidelines and creates the model for data infrastructure governance. This regulation applies to the public administrations and individuals performing public or administrative functions.

The model is composed of political, technical, legal and organisational elements that allow the coordination of actors, agencies, rules, policies, plans, programmes, strategies, methodologies, commitments, processes and procedures to implement, strengthen, manage and handle the data infrastructure to generate public, social and economic value through data.

- Resolution 460 of 2022¹⁰⁵

Resolution 460 of 2022 establishes the National Data Infrastructure Plan. This resolution sets out the guiding principles for the design, implementation and sustainability of the Plan. Principles such as data quality, public trust and ethical data management, standardisation and interoperability, privacy by design and by default, and data security and protection should be highlighted.

Under the Resolution, data infrastructure governance should promote a common understanding of data as infrastructure, coordinating the efforts of the different actors in the data ecosystem, defining recognised single data sources and promoting capacity building of the different actors to adopt common approaches to data.

This regulation applies to the public administrations and individuals performing public or administrative functions. In addition, it establishes that private sector actors, other than those exercising administrative functions, may adhere to the provisions of the Resolution.

Digital Transformation

- National Development Plan 2018-2022 – Law 1955 of 2019¹⁰⁶

The National Development Plan approved for the four-year period 2018–2022 established the obligation for national state entities to include the digital transformation component in their action plans.

Within the framework of this legal instruction, the Ministry of Information and Communications Technologies published the Digital Transformation

¹⁰⁵ Ministry of Information and Communications Technologies. 2022. Resolution 460 of 2022. Available at: https://www.mintic.gov.co/portal/715/articles-198952_resolucion_00460_2022.pdf

¹⁰⁶ Congress of the Republic of Colombia. 2019. Law 1955 of 2019. National Development Plan 2018-2022 Pact for Colombia, Pact for Equity. Available at: http://www.secretariassenado.gov.co/senado/basedoc/ley_1955_2019.html



Framework for the Colombian State¹⁰⁷, which provides tools for public entities to leverage their digital transformation and the use of emerging technologies through the reinvention of processes, products and services.

- Public Policy Document CONPES 3920 of 2019¹⁰⁸

Public policy document CONPES 3920 of 2019 establishes the National Policy on Data Exploitation (Big Data), which aims to increase the exploitation of data, managing it as an asset of great importance that enables public entities to provide more effective goods and services that respond to social needs.

This policy emphasises the need to promote data culture and establish a legal framework that maximises the benefits of data use, ensuring cooperation between the public and private sectors and protecting citizens' rights. It is important to highlight the emphasis placed on the need to distinguish between personal, private sector and public sector data, setting clear boundaries to enhance social welfare.

- Public Policy Document CONPES 3975 of 2020¹⁰⁹

Public policy document CONPES 3975 of 2019 establishes the National Policy for Digital Transformation and Artificial Intelligence. This Policy sees digital transformation as the main driver of the process of generating social and economic value from the strategic use of digital technologies in both the public and private sectors. Thus, the policy addresses the need to remove technological barriers, create conditions for digital innovation, strengthen the skills of human capital and prepare the country for the changes that artificial intelligence will bring.

2- Are there any laws, regulations or provisions specific to sharing or exchanging among government bodies or agencies?

¹⁰⁷ Ministry of Information and Communications Technologies. 2020. Digital Transformation Framework for the Colombian State. Available at: https://mintic.gov.co/portal/715/articles-149186_recurso_1.pdf

¹⁰⁸ National Council for Economic and Social Policy – National Planning Department. 2019. CONPES 3920 of 2019. Available at: <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3920.pdf>

¹⁰⁹ National Council for Economic and Social Policy – National Planning Department. 2019. CONPES 3975 of 2019. Available at: <https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3975.pdf>



Decree 235 of 2010¹¹⁰

Decree 235 of 2010 regulates information sharing between entities for the performance of public functions. Under this rule, entities must implement electronic mechanisms to share or allow access to legally required information, while respecting the right to privacy. It also establishes that bodies must sign contracts defining the terms and conditions for the provision of the required information.

Joint External Circular No. 4 of 2019¹¹¹

The Superintendence of Industry and Commerce and the National Agency for the Legal Defence of the State issued Joint External Circular No. 4 of 2019, which provides instructions to entities of the executive branch and other entities that act as controllers or processors of personal data, in the context of interoperable information systems.

This Circular establishes that institutions may exchange information through interoperable information systems. It clarifies that the circulation of data through these systems must be carried out in accordance with the principles set out in Law 1581 of 2012, taking into account the exceptions set out therein and the rules on the processing and circulation of information.

A) Scope of application within the public sector, and alignment with the above-mentioned laws, regulations, strategies and public policies.

These rules are applicable to all entities of the executive branch, both at a national and territorial level, including individuals exercising administrative functions.

These provisions are in line with the standards set out above, particularly with the provisions of Law 1581 of 2012, which is the statutory regulation that defines the framework for the protection of the fundamental right to *habeas data* and the rules applicable to it.

In the same way, they dovetail with public policies associated with digital transformation.

¹¹⁰ Ministry of Internal Affairs and Justice, Ministry of Finance and Public Credit. 2010. Decree 235 of 2010. Available at: <https://www.suin-juriscol.gov.co/viewDocument.asp?ruta=Decretos/1053347>

¹¹¹ Superintendency of Industry and Commerce, National Agency for the Legal Defence of the State. 2019. Joint External Circular No. 4 of 2019. Available at: https://sedeelectronica.sic.gov.co/sites/default/files/normatividad/122020/40.%20circular_externa_04_5_9_19.pdf



B) Process for sharing data between national government bodies or agencies and local government bodies or agencies.

These provisions are in line with the standards set out above. Particularly with the provisions of Law 1581 of 2012, which is the statutory regulation that defines the framework for the protection of the fundamental right to *habeas data* and the rules applicable to it.

In the same way, they dovetail with public policies associated with digital transformation.

In the Colombian political system, national and territorial entities are generally governed by the same rules. Therefore, territorial or local regulatory provisions cannot go against the provisions of the constitution or nationally applicable laws.

3- Are there any bilateral or multilateral agreements in force that provide for data sharing between states?

With regard to the exchange of tax information, Colombia has signed international treaties that allow the exchange of information with 26 countries under the Convention on Mutual Assistance in Tax Matters¹¹².

It has also signed bilateral agreements with countries such as Spain to exchange information on issues such as the fight against crime, investment and trade between the two countries.

Colombia is also a member of the Pacific Alliance. The agreement of this bloc of nations, composed of Chile, Colombia, Mexico and Peru, promotes the exchange of information and data among them to foster investment, trade and cooperation in economic matters.

Finally, although these are not agreements per se, the Superintendency of Industry and Commerce has defined in Chapter Three of Title V of its Sole Circular¹¹³ the standards required of a third country receiving personal information to have an adequate level of protection. In the same way, it has defined a list of countries with an adequate level of personal data protection. Thus, by virtue of the provisions of

¹¹² Congress of the Republic of Colombia. 2013. Law 1661 of 2013. "Approving the 'Convention on Mutual Administrative Assistance in Tax Matters', made by the depositaries on 1 June 2011 and approved by the Council of Europe and the member countries of the Organisation for Economic Co-operation and Development (OECD)". Available at: http://www.secretariassenado.gov.co/senado/basedoc/ley_1661_2013.html

¹¹³ Superintendency of Industry and Commerce. Sole Circular, Title V. Available at: <https://www.sic.gov.co/sites/default/files/normatividad/092022/T%C3%ADtulo%20V%20Versi%C3%B3n%2029-09-2022.pdf>



Article 26 of Law 1581 of 2012, with the exception of specific exceptions defined in the law, the transfer of data to countries that are not on the aforementioned list is prohibited.

4- Has the State adopted or shown its commitment towards international principles related to data sharing, such as the European Interoperability Framework?

When Law 1581 of 2012 was discussed in Congress, the European Parliament's Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data was used as a reference for issuing this law.

Colombia is committed to the implementation of international principles related to data protection, cross-border information exchange and interoperability through regulatory efforts and public policies.

As a member of the OECD, Colombia is committed to following the Organisation's recommendations on digital governance and data protection.

The Superintendence of Industry and Commerce, in its capacity as the national data protection authority, issued a Guide for the implementation of the Principle of Accountability¹¹⁴, which was updated in 2021¹¹⁵, among other reasons, to refer to accountability in international transfer scenarios. This document takes as a reference, among others, the European Commission's Implementing Decision (EU) 2021/914 on standard contractual clauses for the transfer of personal data to third countries in accordance with Regulation (EU) 2016/679.

5- Other relevant information.

Due to the nature of Law 1581 of 2012 – as it is a Colombian Statutory Law, i.e. it develops fundamental rights – the Constitutional Court carried out a constitutionality check prior to the enactment of the law. In this context, in relation to the transfer of data to third countries, the Court noted the following points in the constitutionality ruling C-748 of 2011:

"It shall be understood that a country has the necessary elements or standards of guarantee to ensure an adequate level of personal data

¹¹⁴ Superintendency of Industry and Commerce. 2015. Guidance for Implementation of the Principle of Accountability. Available at: <https://www.sic.gov.co/noticias/guia-para-la-implementacion-del-principio-de-responsabilidad-demostrada>

¹¹⁵ Superintendency of Industry and Commerce. 2021. Guidance on the implementation of the principle of proven responsibility in international transfers of personal data. Available at: <https://www.sic.gov.co/sites/default/files/files/2021/2021%20Gu%C3%ADas%20para%20implementaci%C3%B3n%20del%20principio%20de%20responsabilidad%20demostrada%202021.pdf>



protection if its legislation has principles covering the obligations and rights of the parties (data subject, public authorities, companies, agencies or other bodies that process personal data) and of the data (data quality, technical security), and a data protection procedure involving mechanisms and authorities that make the protection of information effective. It follows that the country to which the data is transferred cannot provide a lower level of protection than that provided for in this body of regulations under study.”¹¹⁶

¹¹⁶ Constitutional Court of Colombia. 2011. Ruling C-748 of 2011. Available at: <https://www.corteconstitucional.gov.co/relatoria/2011/c-748-11.htm>