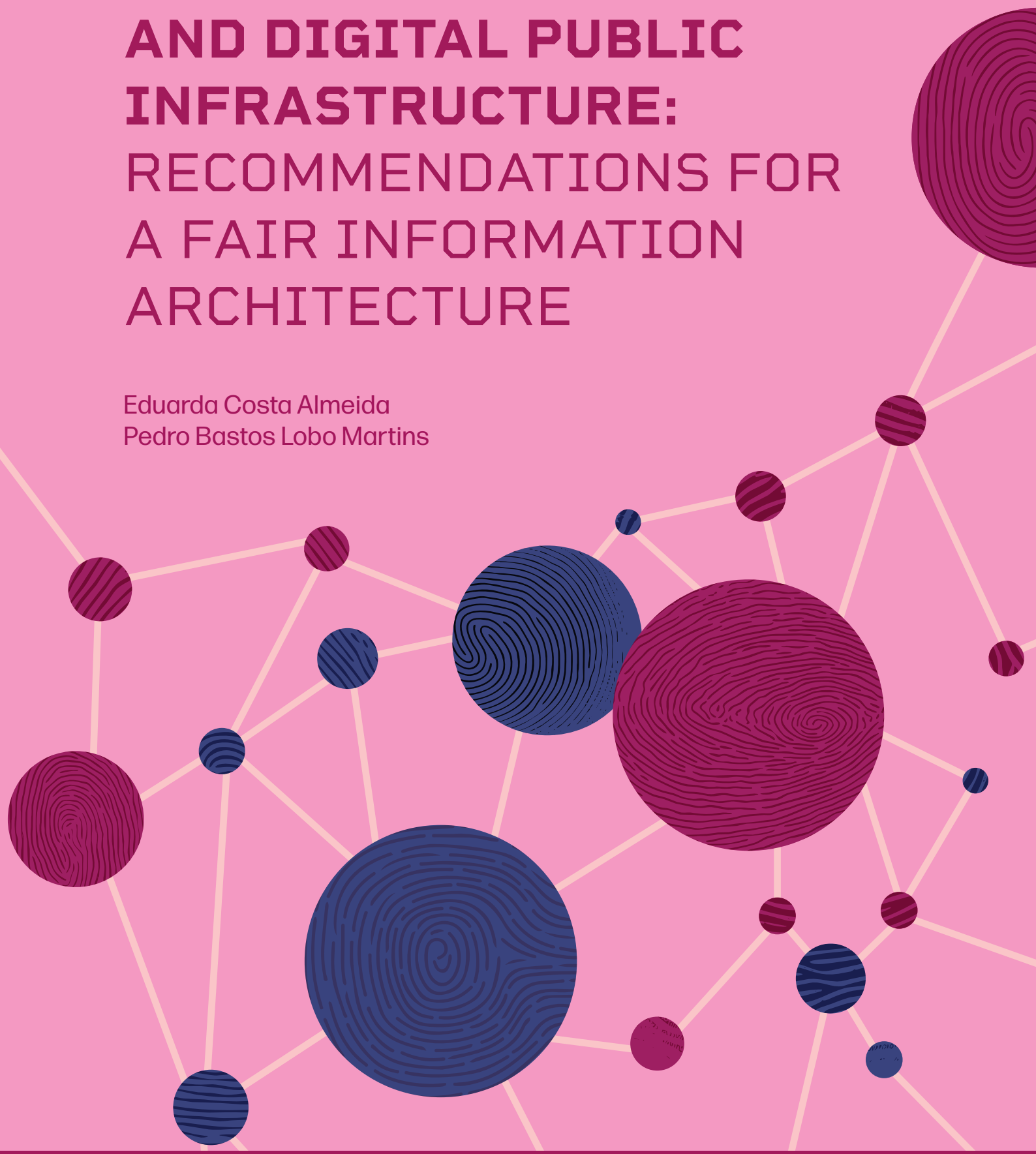
DIGITAL IDENTITY AND DIGITAL PUBLIC INFRASTRUCTURE: RECOMMENDATIONS FOR A FAIR INFORMATION ARCHITECTURE

Eduarda Costa Almeida
Pedro Bastos Lobo Martins



DataPrivacyBR Research

SUPPORTED BY
ripple

About Data Privacy Brasil

Data Privacy Brasil is an organization that was born from the union between a school and a civil association to promote a culture of data protection and digital rights in Brazil and around the world.

Founded in 2018, Data Privacy Brasil Ensino emerged as a space to disseminate and innovate knowledge about privacy and data protection in the country. With content adapted to a more practical language, with exercises and case studies, this is a school for all those who are interested and want to delve deeper into the rich themes of privacy, data protection and new technologies.

The Data Privacy Brasil Research Association is a non-profit, non-partisan civil society organization that promotes the protection of personal data and other fundamental rights from a perspective of social justice and power asymmetries.

As of 2023, the two institutions will join forces to form a single organization, maintaining the same principles and activities. With the support of a multidisciplinary team, we provide training, events, certifications, consultancy, multimedia content, public interest research and civic audits to promote rights in a data-driven society marked by asymmetries and injustices. Through education, awareness raising and mobilization of society, we aim for a democratic society where technologies are at the service of people's autonomy and dignity

www.dataprivacy.com.br | www.dataprivacybr.org

Directors

Bruno Bioni, Mariana Rielli e Rafael Zanatta

Coordinators

Carla Rodrigues, Jaqueline Pigatto, Pedro Martins, Pedro Saliba e Victor Barcellos

Team

Alicia Lobato, Barbara Yamasaki, Eduarda Costa, Eduardo Mendonça, Gabriela Vergili, Giovana Andrade, Isabelle Santos, Johanna Monagreda, João Paulo Vicente, Larissa Pacheco, Louise Karczeski, Matheus Arcanjo, Natasha Nóvoa, Nathan Paschoalini, Otávio Almeida, Pedro Henrique, Rafael Guimarães, Rennan Willian, Rodolfo Rodrigues e Vinicius Silva.

Licence

Creative Commons

The use, circulation, expansion, and production of derivative documents are free as long as the original source is cited and for non-commercial purposes.

Press

For clarifications about the document and interviews, please contact us at imprensa@dataprivacybr.org

How to cite this document

ALMEIDA, Eduarda Costa; MARTINS, Pedro Bastos Lobo. Digital Identity and Digital Public Infrastructure: recommendations for a fair information architecture. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2025.

Executive Summary

This report examines the impact of a Digital Public Infrastructure (DPI), especially digital identity applications, on the protection of personal data in the light of the Brazilian Federal Constitution (FC) and the General Data Protection Law (LGPD). The aim is to understand how the DPI and digital identity ecosystem relate to, tension and shape the exercise of fundamental rights, particularly through the lens of data protection as an eminently procedural right, which aims to establish parameters to ensure that the flow of information in the DPI is fair and promotes rights.

The growing digitalization of society and government services requires the creation of a robust and reliable DPI so that people can interact securely with the infrastructure's applications. In this sense, the digital identity acts as the gateway to the DPI, and therefore plays a crucial role in accessing essential services and products. However, the use of personal data in digital identity systems raises significant concerns about data protection, self-determination and the potentialization of existing inequalities.

Given the complexity of this scenario, this report serves as an essential tool for building an DPI that promotes a flow of data, including personal data, that is fair, inclusive and respects the fundamental right to data protection. The report is a call to action for governments, the private sector and civil society, emphasizing the importance of multi-stakeholder collaboration to ensure that DPI is an instrument of social development and public value, and not a tool of control or exclusion.

From a data protection perspective on DPI identity applications, the following conclusions can be drawn:

- **Data protection is an autonomous fundamental right in Brazil, recognized by the Supreme Court and the Federal Constitution, and must be considered in the design, development and implementation of digital identity systems in the DPI.** This does not mean the simple collection of consent for any processing carried out in the DPI, informational self-determination, contextual data protection and the informational separation of powers, themes that are explored in depth in this report.

- **Generating public value is a condition of a DPI. There is only DPI when the common good and the public interest are guaranteed.** Ensuring that DPI applications meet the goals and directions of this community guarantees the legitimacy and sustainability of the results achieved. Simply generating economic value from data does not guarantee the achievement of public value if the rights of individuals are neglected.

- **Identifying public value requires an understanding of what the community defines as the "common good".** This process must be contextualized and continually updated, taking into account the specific principles, needs and objectives of each community over a given period of time through civic participation mechanisms. This infrastructure must be designed and implemented in such a way that it is interoperable and benefits society as a whole, not just private interests or specific sectors, allowing the different systems and actors that make up the DPI to exchange data in an appropriate manner, without this infrastructure being captured by a single or group of actors.

- **Digital identification processes are constantly changing, so the risks associated with a digital identity are not just the sum of the risks of identity and its digitization.** Identification processes can vary in their degree of robustness and application context. With technological advances, a layered identity model has been developed, where multiple identity systems integrate and communicate. In addition, in complex processes, authentication is based on probabilistic models based not only on data provided by the holder, but also on correlations and inferred data. This intense flow of data can strain the compatibility between the purpose of collection and subsequent uses, of which the data subject is unaware and has little power of self-determination, requiring adequate safeguards so that secondary uses are compatible with the normative values of data protection.

- **Informational autonomy and self-determination ensure that individuals are able to exercise their capacity to develop their personalities freely,** without being subjected to forms of social control that nullify their individuality. Data subjects must have free access to personal data and to clear, accurate and easily accessible information about how their data

is being used, so that they can question and object to processing they do not agree with. These rights allow the flow of data to be co-constructed with the data subject, which can generate higher quality databases and even act as barriers to fraud and identity theft.

- **The concept of privacy as contextual integrity is crucial to guaranteeing a fair flow of information in digital identity systems.** Data protection is preserved when data is treated in accordance with the reasonable expectations of the data subjects, taking into account the specific context in which it is collected and used, the person to whom the data refers, the entity sending the data and the one receiving it, as well as the nature of the data shared.

- **The principle of the informational separation of powers must be applied to identity systems in the DPI.** The flow of data between state bodies must be limited to their specific competencies and purposes, avoiding the concentration of power and misuse of purpose. Sharing must serve a specific purpose that meets public value, so that processing is conditional on there being a legitimate reason for the other body to receive the data, and formal administrative procedures must be put in place, in addition to using electronic security and access registration systems.

- **The implementation of data protection and accountability mechanisms is essential to guarantee a public value to DPI, as well as promoting trust and security in the infrastructure.** Data protection, in this context, is not limited to secrecy and information security, but seeks a secure and adequate data flow, with a fair and participatory information architecture. This includes compliance with data protection principles, the rights of data subjects, and multisectoral participation in the construction and maintenance of this infrastructure.

- **In the DPI, consent is understood as one of the legal bases justifying data processing, but it is not the only one, nor is it always the most appropriate.** This occurs, for example, when data is processed in order to operationalize public policies, generate data to evaluate the effectiveness of policies, promote public transparency or monitor compliance

with regulations. In these cases, consent cannot be considered free, since the processing is necessary to meet legal obligations or the interests of other agents, such as the state. In addition to consent, data protection tools act as catalysts for a fair flow of information, guaranteeing other legal bases to justify the processing of data in a legitimate manner and with the appropriate guidelines and safeguards.

- **Defining areas of responsibility in the development of DPI avoids insecurity and strengthens confidence in the infrastructure and its applications.** Clarity in defining the responsibility of each agent is fundamental so that users know who to turn to in the event of damage. DPI involves multiple actors collaborating in the same ecosystem. Without the definition of responsibilities and accountability mechanisms, there can be uncertainty about the rules common to all actors when there is a need to repair damage.

- **The active participation of different sectors of society is fundamental to the development of a fair and citizen-based DPI, ensuring that identity systems serve the public interest.** By enabling co-creation spaces, communities can actively influence the design, implementation and monitoring of these infrastructures. Holding public consultations, implementing whistleblowing channels and creating an independent oversight board are important measures to promote participation.

In short, building a fair, ethical and public interest-oriented DPI requires a **collaborative approach** involving the public and private sectors, civil society and academia. The implementation of data protection and accountability tools, as well as participation in this process, is essential to ensure that DPI is useful, efficient and in line with the values of society as a whole. Assessing risks, establishing rules, listening to society, being transparent and open to public scrutiny generates a public policy that is more assertive from the outset and geared towards meeting society's demands. In this perspective, this report contributes to the public debate on DPI in Brazil, offering subsidies for the formulation of public policies that promote innovation, digital inclusion and respect for fundamental rights at the same time.

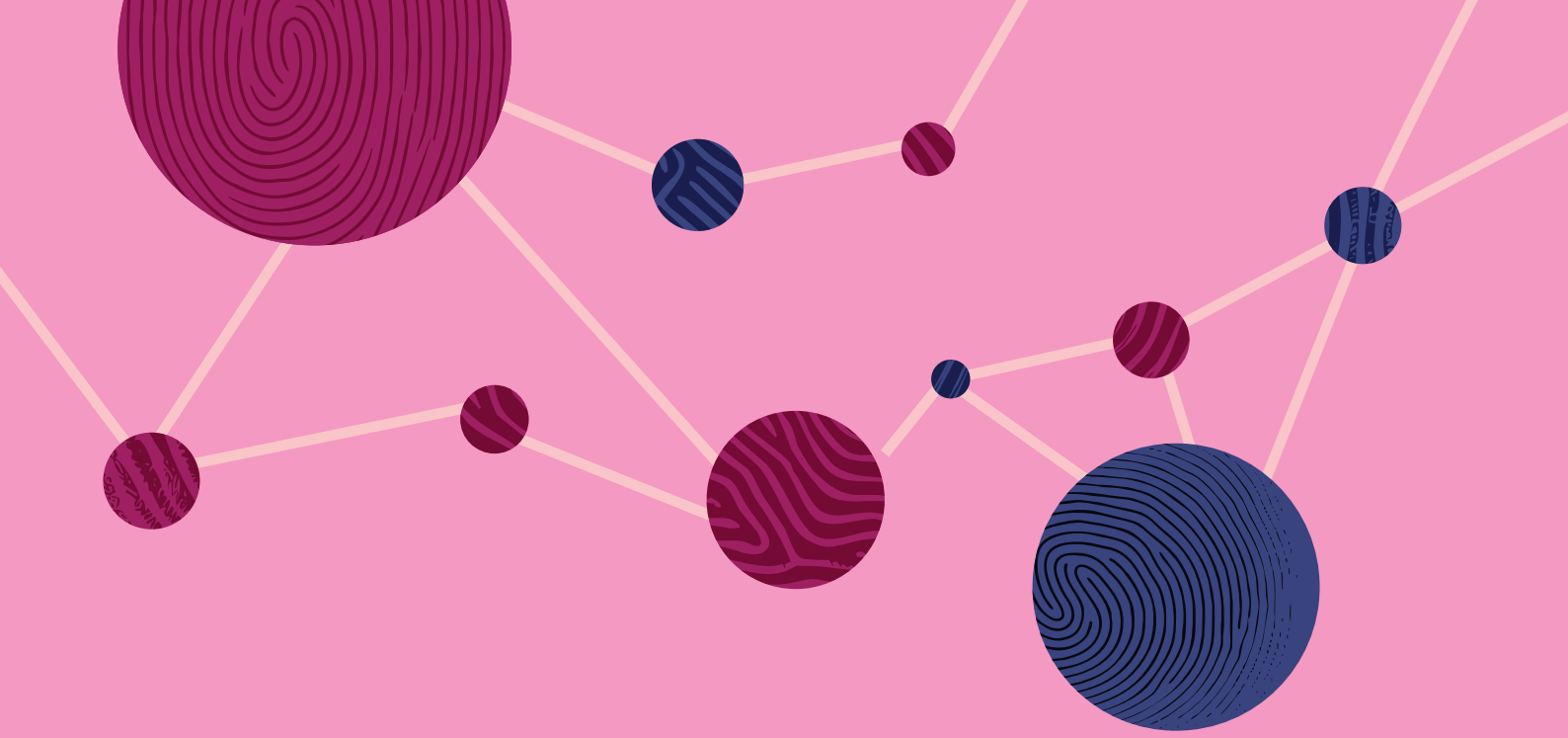
Acknowledgement

This research was supported by Ripple. The study was enriched by interaction with a community of experts and professionals who have played a key role in the debate on IPD in Brazil.

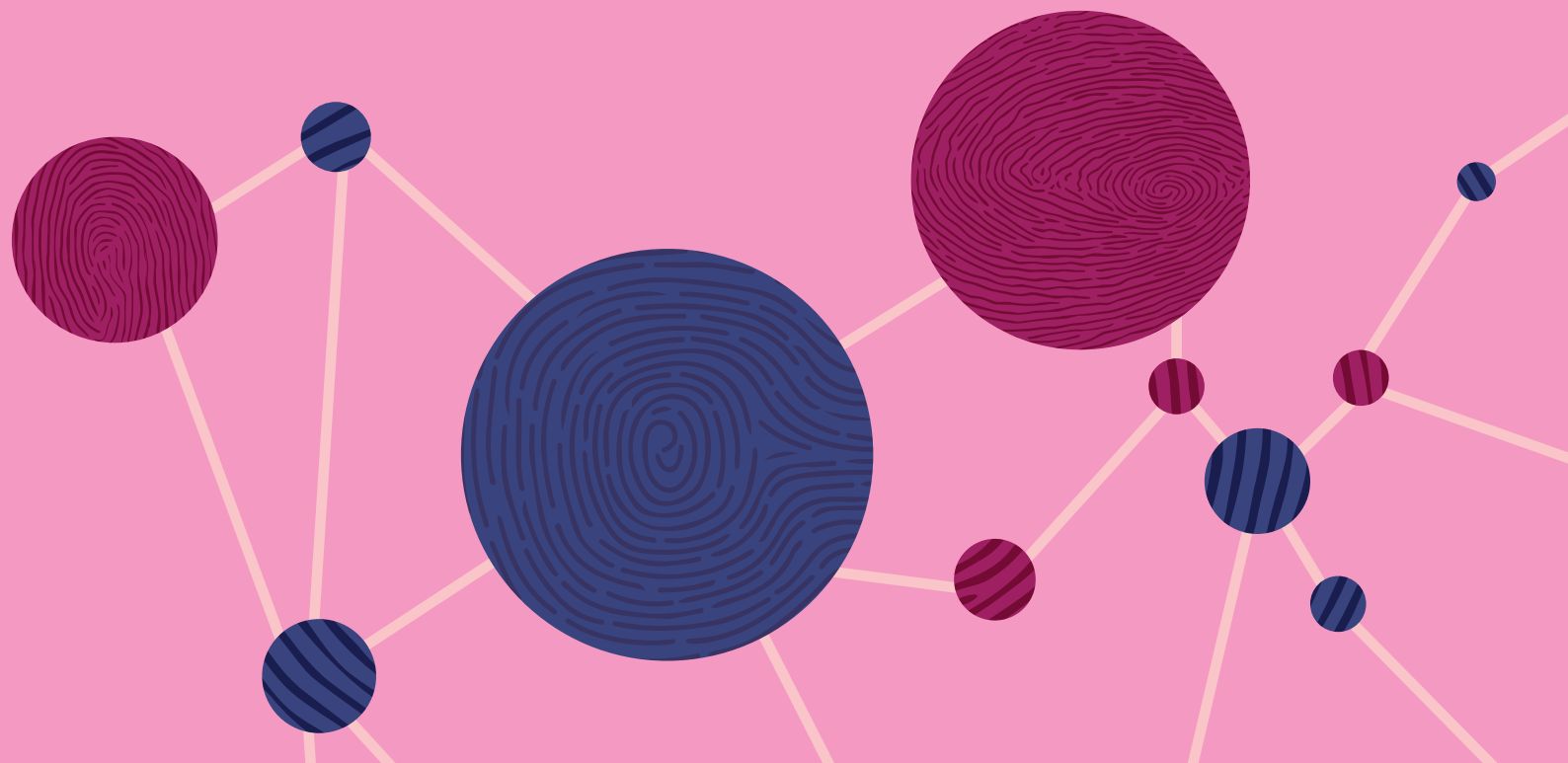
We would like to thank all those involved in the preparation of this report, especially in the initial field mapping interviews, for their fundamental contributions to deepening the subject, as well as their open dialog and collaboration throughout this project. We would also like to thank the specialists Maria Luciano, Igor Gonçalves and Hudson Mesquita for their commitment and support in discussing the results and critically reviewing the final version of the text.

We would also like to express our gratitude to the professionals who work directly in the field, whose experience and perspectives were essential to the development of this research. In particular, we would like to thank all the participants in the Digital Identity track for their participation in the event "Common Horizons: the role of digital public infrastructure in finance, identity and climate justice" held on April 30, 2024 and organized by Data Privacy. We thank the participants for their generosity in sharing their knowledge and reflections.

INDEX



01.
INITIAL CONSIDERATIONS



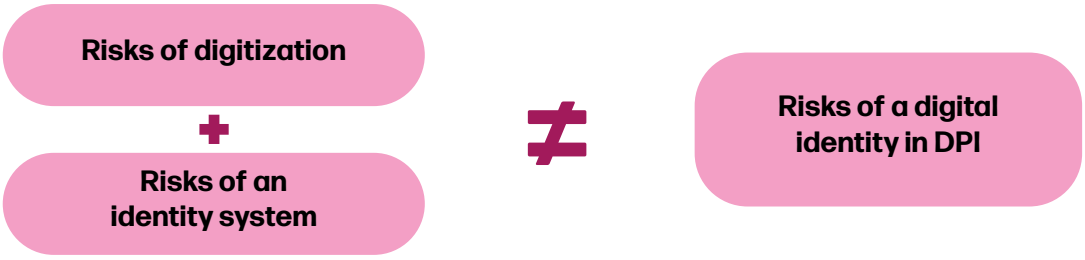
1 Initial considerations

Technology has profoundly transformed human interactions, shifting everyday processes from analog to digital, including identification tools. These digital identification processes have become central to access public and private services, authenticating transactions and mass participation in the digital economy, when necessary.

However, the massive use of identification processes also amplifies the risks associated with the misuse of personal data, mass surveillance and digital exclusion. Data governance thus emerges as a crucial element in balancing the appropriate use of technological advances with the protection of fundamental rights. Robust governance therefore seeks to ensure that digital identification processes respect privacy, promote inclusion and strengthen citizens' trust in digital infrastructures so that DPI can be another facilitating tool available to people.

1.1. Digital Public Infrastructure

Starting from the framework of a digital public infrastructure (DPI), this report looks at the obstacles faced in guaranteeing the right to data protection from the design to the implementation and monitoring of digital identity systems. This is because identity systems in DPI present risks to people that go beyond the sum of the risks of an identity system and its digitization considered separately.[1]



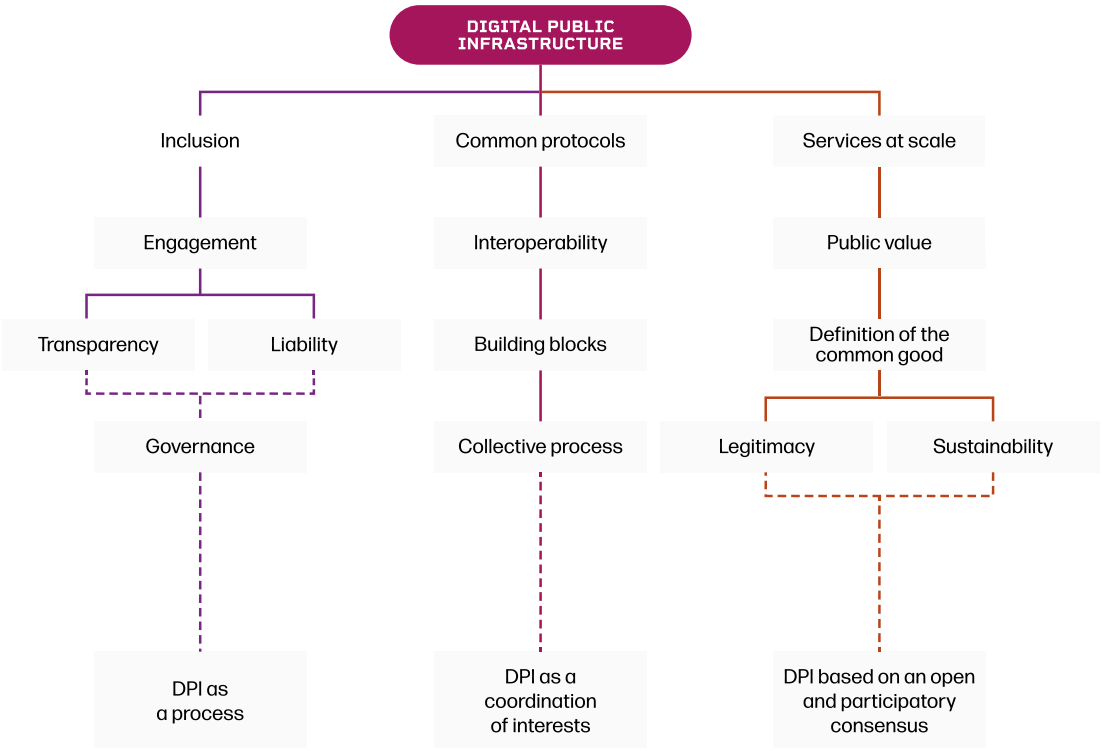
Just like physical infrastructure, the development of a DPI is a possible way to guarantee the functioning of an organization in accordance with common good, now also available in the digital environment. It is the infrastructure that guarantees the availability of resources to support productive activities and promote

1 ALMEIDA, Eduarda Costa; MARTINS, Pedro Bastos Lobo. A Infraestrutura da identidade: os influxos de uma identidade digital como aplicação da IPD. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2024.

social development[2].

As a result, infrastructure applications are more useful as components of an ecosystem made up of other applications, as is the case of identity solutions. These identity applications are fundamental elements of DPI because they guarantee the identification of the user of the infrastructure and, thus, allow them to access any DPI application in a secure and convenient way.

Although there is no unique definition of the concept of DPI, this report assumes that DPI is a process built on the coordination of interests and an open and participatory consensus. In this sense, an DPI is defined as bringing together common protocols, interoperability, public value, the common good, inclusion and participation through a collective process.



2 CARVALHO, A. C. Infraestrutura sob uma perspectiva pública: instrumentos para o seu desenvolvimento. 2013. 608 f. Tese (Doutorado em Direito) - Faculdade de Direito, Universidade de São Paulo. p. 86.

As a backdrop for the development of identity applications, the notion of DPI mobilizes some key concepts to understand the frames of this digitization process, such as **infrastructure**. This element is, by its nature, vague and has various uses, because infrastructure is the foundation that is used to build other applications[3]. Traditional examples of infrastructure are transportation systems, including roads, railroads, airports and ports, as well as telecommunication, water and sanitation systems.

The sense of infrastructure is also associated with the building blocks approach, where applications can be added on top of a common base, changes can be accommodated and the functionality of the infrastructure increased, allowing for updates and improvements whenever necessary. Infrastructure solutions, as a rule, are managed in an open and accessible way, so that all members of a community who wish to use its resources can do so on equal and non-discriminatory terms, even if access is not free[4].

In addition, infrastructure changes are known to generate significant spillovers, positive externalities, which result in large social gains. The traditional idea of infrastructure was derived from the observation that the private gains from building and expanding transportation and communication networks were also accompanied by large additional social gains.[5]. In this sense, the very notion of infrastructure is linked to the production of value that is beneficial to the agents who produce it, but also to the users who access it, an idea that will be highlighted in this report.

When designed for the DPI context, any infrastructure must allow the entities participating in it to interact freely [6] and build independent modules. The construction of this infrastructure is mainly the result of the technology used for it. Therefore, in order for this technology to meet these infrastructure requirements, it is essential

---

3 ZUCKERMAN, Ethan. What Is Digital Public Infrastructure? Center for Journalism and liberty, 17 nov. 2020. Disponível em: https://www.journalismliberty.org/publications/what-is-digital-public-infrastructure. Acesso em: 27 abril 2024.

4 FRISCHMANN, Brett M., Defining Infrastructure and Commons Management. In: FRISCHMANN, Brett M. Infrastructure: The Social Value of Shared Resources, p. 3, Oxford University Press, 2012, Available at SSRN: https://ssrn.com/abstract=2117460. p. 4

5 FRISCHMANN, Brett M., Defining Infrastructure and Commons Management. In: FRISCHMANN, Brett M. Infrastructure: The Social Value of Shared Resources, p. 3, Oxford University Press, 2012, Available at SSRN: https://ssrn.com/abstract=2117460. p. 5

6 PORTEOUS, David. Is DPI a useful category or a shiny new distraction? 2023. Disponível em: https://www.integralsolutionists.com/is-dpi-a-useful-category-or-a-shiny-new-distraction. Acesso em: 27 abril 2024.

that it reflects other elements, such as scalability, extensibility, openness and interoperability.[7].

Developing a DPI using common protocols allows other functionalities to be added to it and these can interact with each other. The exchange of information between infrastructure applications, regardless of their origin, may generate trust and facilitate the secure flow of data. At the same time, the DPI must be able to increase its capacities and functionalities efficiently as demand arises, without compromising the performance or quality of the services offered.

These DPI elements are translated into identity applications that must be recognized by a significant number of agents in the DPI ecosystem, making the solution extensible and scalable. Also, in line with interoperability, identity information and its validation must be able to move through systems, even if they are in different applications. In other words, different systems must be able to communicate with each other based on the definition of common and reliable standards.

Public value is also one of the key elements of DPI. This means that DPI applications should serve the common good by maximizing public value[8]. However, defining what is the common good is a contextual process and varies according to the principles, needs and objectives of each community. From the delineation of what is the common good, the idea of public value takes on a specific object and direction. For this reason, there is still a lot of dispute over the meaning of public value in DPIs. As an example, in the Brazilian context, the public value of DPI was presented as public interest, one of the essential elements of DPI, by Decree No. 12,069 of June 21, 2024.

It is essential that DPI applications meet the aims and directions of the community in which they are located. This understanding not only directs DPI construction efforts towards concrete demands, but also guarantees the legitimacy and sus-

7 UNDP. The DPI Approach: A Playbook. 21 ago. 2023. Disponível em: https://www.undp.org/publications/dpi-approach-playbook. Acesso em: 27 mar. 2024.

8 MAZZUCATO, Mariana; EAVES, David; VASCONCELLOS, Beatriz. Digital public infrastructure and public value: What is 'public' about DPI? UCL Institute for Innovation and Public Purpose, Working Paper Series (IIPP WP 2024- 05). Disponível em: https://www.ucl.ac.uk/bartlett/public-purpose/publications/2024/mar/digital-public-infrastructure-and-public-value-what-public-about-dpi. Acesso em: 25 abril 2024.

tainability of the results achieved[9]. Thus, the coordination of interests in the process is essential to ensure that diverse perspectives are considered, promoting an open and participatory consensus on what constitutes public value.

Unraveling what public value means for a community presupposes the inclusion and participation of the entities that make it up. This is because only by getting to know their needs and aspirations is it possible to design a foundation that is useful for a society. It's worth noting that the definition of public value isn't just set by one group that makes up society and is accepted by the others, it's the result of a diverse and collective process in which there are spaces for co-creation and effective participation.

For the public value element to be met by DPI, society must have formal and material tools to influence the development of its applications, as well as their implementation and monitoring. This participation is fundamental to driving innovation and creating solutions centered on people and the diversity of the groups that make up this community. This collaboration aims to ensure that the benefits of public value are distributed equitably, generating inclusive growth and sharing the knowledge and skills developed in the process[10].

Furthermore, the process of identifying the common good involves implementing transparency and accountability tools in order to build and maintain the community's trust in the infrastructure[11]. Based on these elements, it is possible to control and monitor the actions implemented by the entities that make up the DPI, ensuring that society has useful information and tools to understand how the public value is being met or not by the DPI.

It is also important that the frames of this public value are revisited and defined in a process that undergoes updates. It is important that the changing interests of society are reflected in the definition of the common good and public value, and thus impact the direction of DPI applications. It is in this sense that the development of DPI

---

9 MAZZUCATO, Mariana. Governing the economics of the common good: from correcting market failures to shaping collective goals. Journal of Economic Policy Reform, 27(1): 1-24, 2023. DOI: 10.1080/17487870.2023.2280969

10 MAZZUCATO, Mariana; RYAN-COLLINS, Josh. Putting value creation back into "public value": from market-fixing to market-shaping. Journal of Economic Policy Reform, 25(4): 345-360, 2022. DOI: 10.1080/17487870.2022.2053537.

11 UNDP. The DPI Approach: A Playbook. 2023. Disponível em: https://www.undp.org/publications/dpi-approach-playbook. Acesso em: 27 mar. 2024. p. 11.

and its applications should be understood as a process of coordinating interests based on open and participatory elaborations.

In view of the DPI's transformative potential, several countries and international organizations have been looking into the subject in order to create c**oncepts and consensus** for coordinated implementation and mutual learning about the impacts of the DPI. The G20 is one of the places where this discussion has been most fruitful, especially under the presidency of India, Brazil and South Africa.

Taking into account the impact of digitization processes, the Brazilian Federal Government has drawn up the Federal Digital Government Strategy[12] eand the National Digital Government Strategy[13], mentioned in Law No. 14.129[14]. The national strategy was published as Decree No. 12.069 of 2024, responsible for guiding the digital transformation of municipal, state and federal governments, articulating and boosting digital government initiatives throughout the country, considering their breadth and diversity, as well as reducing regional inequalities and improving access to public services[15].

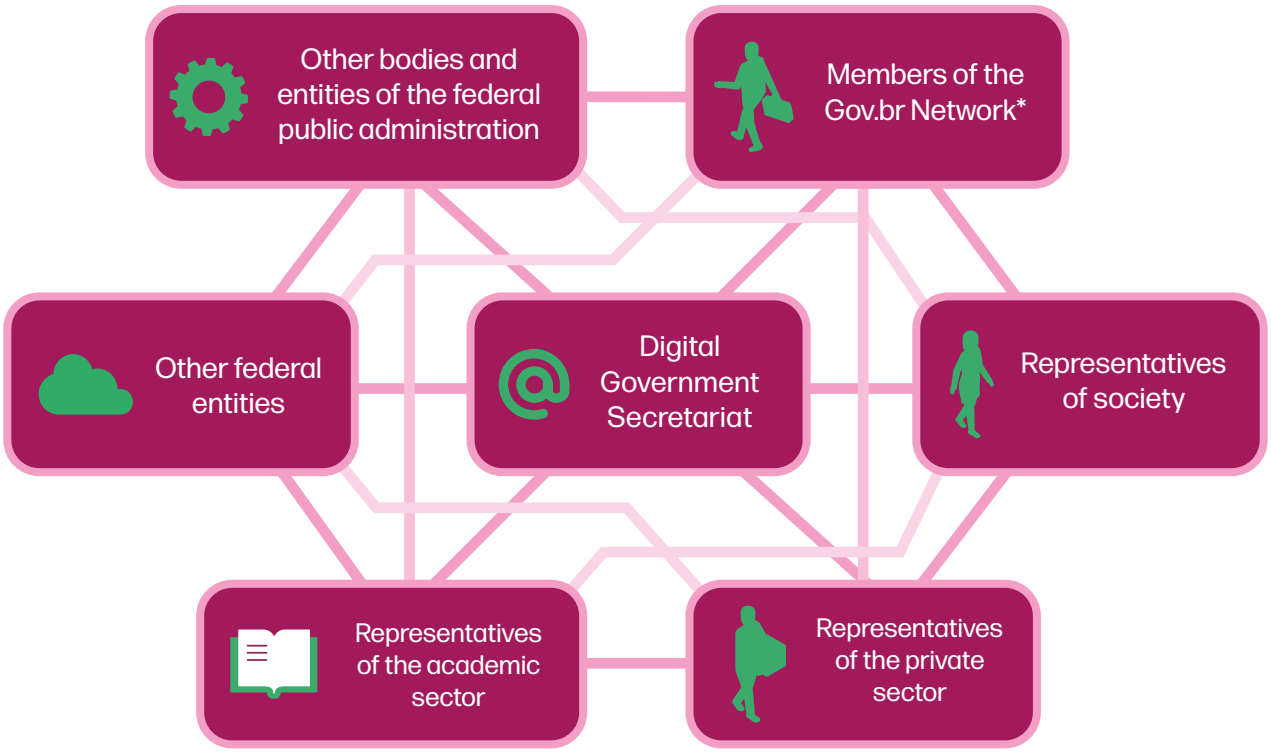
This Decree designates the Digital Government Secretariat (*Secretaria de Governo Digital - SGD*) as responsible for promoting the development, implementation and use of DPIs, in conjunction with various other agents, namely:

12 MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. Estratégia Federal de Governo Digital 2024-2027. Governo Digital. Disponível em: <https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/EFGD>. Acesso em: 7 nov. 2024

13 MINISTÉRIO DA GESTÃO E DA INOVAÇÃO EM SERVIÇOS PÚBLICOS. Estratégia Nacional de Governo Digital. Governo Digital. Disponível em: <https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-digital/estrategianacional>.

14 Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/L14129.htm. Acesso em: 07 nov. 2024.

15 BRASIL. Ministério da Gestão e Inovação. Consulta Pública - Estratégia Nacional de Governo Digital. Brasília, 15 dez. 2023. Disponível em: https://dados.gov.br/dados/conteudo/consulta-publica-estrategia-nacional-de-governo-digital



* Made up of federated entities that have joined the network by means of an Adhesion Agreement signed by the highest authority of the Executive Power at state, district or municipal level[16].

This shows a formal openness on the part of the SGD for other entities to be heard in the process of developing a DPI. This determination is directly aligned with the notions of public participation, a key element of a DPI.

The Decree also dialogues with other DPI elements regarding infrastructure **priorities**, which can be compared as follows:

16 BRASIL. Ministério da Economia. Portaria nº 23, de 4 de abril de 2019. Disponível em: https://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/70491912/do1-2019-04-08-portaria-n-23-de-4-de-abril-de-2019-70491574#:~:text=Disp%C3%B5e%20sobre%20diretrizes%2C%20compet%C3%AAncias%20e,vista%20o%20disposto%20no%20art. Acesso em 03 de set. de 2024.

DPI priorities according to the Decree	Related DPI elements
The search for universal access to DPI's functionalities, with a focus on innovative and inclusive technological solutions centered on people's needs.	Infrastructure that is scalable, extensive, open, public, inclusive and geared towards public value.
The adoption of technological standards that are interoperable, secure, scalable and economically sustainable in the long term.	Interoperable, scalable and sustainable infrastructure.
The promotion of secure data sharing, active transparency and environmental sustainability, under the terms of the law.	Targeting public value, with parameters of transparency and accountability.
The integration of digital and physical channels.	Interoperable and scalable infrastructure, without abandoning the solutions available on physical media[17].
The prior mapping of risks and the taking of measures to mitigate them, in order to guarantee the adoption of privacy, data protection and information security practices throughout the DPI lifecycle.	Responsibility parameters.

Furthermore, Decree No. 12,069 recognizes as DPI for civil identification the set of initiatives of the Citizen Identification Service (*Serviço de Identificação do Cidadão*) and the Gov.br Platform, specifically with regard to the electronic signature tool in interactions with public entities and the user's unique digital access mechanism to public services, with a level of security compatible with the degree of demand, nature and criticality of the data and information pertinent to the public service requested[18].

1.2. Digital Identity

One of the pillars of DPI is the digital identity. This form of identity is the result of registering a set of unique electronic attributes to meet three traditional, dependent and convergent functions: identification, authentication and authorization.

For an identity to fulfill the **identification** function, credentials must be issued based on the collection of biographical information. Thus, a person becomes identifiable

17 UNDP. The DPI Approach: A Playbook. 2023. Disponível em: https://www.undp.org/publications/dpi-approach-playbook. Acesso em: 27 mar. 2024. p. 13.

18 BRASIL. Decreto nº 8.939, de 19 de dezembro de 2016. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8936.htm#art3ix. Acesso em 03 de set. de 2024

upon the presentation and validation of these credentials. It is with identification that it is possible to prevent any type of duplication in the issuing of the credential.

This stage is critical, because if there is any barrier or friction in it, the next functions are impaired. If a person is not identified, they cannot have their identity validated and, consequently, they cannot access spaces or services intended for people who have gone through the identification process.

The other two functions of identity start from the assumption that it has been possible to identify a person, and this unlocks the activities of authentication and authorization. **Authentication** is the function of confirming or rejecting that a person is who they say they are. As a rule, this verification is based on factors that the person holding a given identity claims to have, know or be, or even a combination of more than one factor.

From the authentication of the identity carried, the person to receive authorization to access specific products or services, appropriate and limited to their level of access. Thus, given these identity functions, it is possible for entities that need to identify people to confirm, either during the initial integration of a newly identified person, or on an ongoing basis, that the person is eligible to access a certain right, service, information or system functionality.[19]. In this way, it is clear that the functions of identity systems are exercised at different times to guarantee trust in the application used.

19 WORLD BANK. ID4D Practitioner's Guide: Version 1.0. Washington: World Bank License, out. 2019, p. 20. Disponível em: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf. Acesso em: 28 jan. 2024.

Additional information

Digital ID's attributes[20]

A type of digital identity can be a file in a digital wallet that stores various pieces of trusted information about someone, i.e. their attributes. In this scenario, the subject can choose when and with whom to share it, without having to share the entire digital wallet. This could include disclosing personal data, such as legal name, date of birth, address, place of work or study, as well as details from other organizations, such as their professional qualifications or employment history.

Another type of digital identity can provide authentication of an internet user when people need to prove their identity to a third-party organization. It is possible for a person to securely log in to their identity service provider and thereby authorize the sharing of appropriate information with the third-party organization. For example, when a person buys age-restricted products from an online retailer without telling their age, but only by proving that they are over 18.

Digital identities can also be used on the internet to prove who is involved in a transaction. They would eliminate the need to send copies of documents to prove who people are, with all the risks of data being lost or stolen. Instead, people could use a digital identity to prove something about themselves. It would also be possible to use digital identities to ensure that the person or organization you are dealing with is who they say they are before sharing any information.

In general, the aim of digital ID is to put people in control of what and how much information they manage and share. It provides a way to protect personal data and can prevent organizations from obtaining information that the person would rather not share.

20 .UK. UK Digital Identity and Attributes Trust Framework Alpha v1 (0.1). GOV.UK. Disponível em: https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework#introduction. Acesso em: 2 dez. 2024.

One of the fundamental pillars of the transformation driven by DPI is the implementation of a digital identity. DPI and digital identity have a very intertwined relationship: DPI provides the technological and governance basis necessary for digital systems and services to function, while some of the infrastructure's applications can only work if it is possible to identify the user in a secure and convenient way.

As part of our relationships become digital, the challenge of knowing with whom these relationships and obligations are being entered into takes on a new dimension. In other words, in some cases it becomes relevant to know if the person behind the screen is really who they say they are. In some applications, identity is the gateway to the digital world, which increases the demand for a robust and reliable validation process.

Identity solutions are not necessarily to be confused with *logging in or signing on* to a website. Unlike these processes, identity is intended to be unique[21] and is restricted to real people only, which may not be the case in other systems. [22].

Depending on the context, identification processes can vary in their degree of robustness. Although they aim to identify, it is not common for a simple online purchase to verify the identity of the consumer through a document issued by the state. At the same time, in the case of a bank transfer, there is an expectation that certain security and integrity requirements will be guaranteed in order to confirm the identity of those involved in the process.

In this way, authentication and even identification processes have become increasingly complex, so that identity is now based not only on personal data provided by the subject, but also processed through sharing and cross-referencing data from other sources.

---

21 OECD. OECD/LEGAL/0491. Recommendation of the Council on the Governance of Digital Identity. 8 jun. 2023. Disponível em: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491. Acesso em: 27 jan. 2024.

22 GOV.UK. UK Digital Identity and Attributes Trust Framework Alpha v1 (0.1). GOV.UK. Disponível em: https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework#introduction. Acesso em: 2 dez. 2024.

First Thoughts

Layered identification and authentication

With the complexification of identity processes, authentication is no longer understood simply as verifying a person's identity, validating that they are who they say they are based on the information they present. Authentication mechanisms now influence identification itself. In other words, authentication becomes a process of *disclosure* (unveiling through sharing) of personal information between an identified person and the agents of the identity ecosystem they aim to identify.

This *disclosure* allows for the complexification of the identity process, no longer just validating someone's identity based on the biographical data recorded on a credential, but authorizing, for example, a financial transaction based on the lack of evidence of fraud from other personal information and behavioral patterns collected by other agents in different contexts and for different purposes.

The intense flow of data is related to a **layered identity** model, in which there is the integration of multiple identity systems, which the subject relates to individually, in specific contexts and for specific purposes, but these systems add up and communicate to form layers of someone's identity. These layers stress the compatibility between the purpose of the collection and subsequent uses of which the subject is unaware.

One of the challenges faced in developing identity as a DPI is maintaining and promoting the autonomy of the people identified. With the integration of the grassroots and the exchange of information between different agents, people gradually lose their **power of intentional agency** over themselves, thus losing the ability to self-identify and be authoritative in their actions, individually or collectively[23].

23 ROUVROY, Antoinette. The end(s) of critique: data behaviourism versus due process. In: HILDEBRANDT, Mireille; DE VRIES, Katja (eds.). Privacy, Due Process and the Computational Turn: the philosophy of law meets the philosophy of technology. NewYork: Routledge, 2013. p. 143-167.

The **ecosystem of agents** that work on identity solutions also becomes complex and the identity provider is no longer the only agent that can validate them. This is because the data that makes up the identity is not necessarily only that collected by the provider at first. Data other than that of the identity provider can make up someone's identity. Furthermore, relying parties and entities can authenticate the credentials issued to a subject even without direct dialogue with the provider, but only on the basis of other identification data from other sources.

In the traditional model, identification was based on a binary logic: a person's identity was validated as "yes, they are the subject of the credential they are presenting" or "no, they are not the subject of the credential they are presenting", based on information provided directly, such as a document or password.

However, in these complex processes, the logic is based on a probabilistic model, i.e. authentication is no longer based on direct validation, but on confidence percentages calculated from various data and correlations. For example, a system can conclude that there is a 92% chance that a person is who they say they are, based on cross-checking information such as online behavior patterns, biometrics and geolocation.

In this scenario, there is a prevalence of the **sharing** and cross-referencing of personal data collected by the most diverse agents, in a variety of contexts and for a variety of purposes. A more intense flow of data means that the attribution of a characteristic to a person can also be easily transmitted and used in other identification processes unrelated to the initial one. In a DPI, this process reaches significant scales, increasing the potential risks associated with this logic of sharing, including allowing these risks to be transmitted between different identification systems.

Hypothetical example

Identity as a result of probabilistic analysis

Maria lives on the outskirts of São Paulo and is looking for a loan to open her small sewing business. She works informally and relies on her social networks to sell her clothes and interact with potential customers. As part of her daily life, she also shares details about her personal life, including posts

about temporary financial difficulties and health problems she has faced in the past. Maria uses her daughter's bank account to receive transfers relating to payments for the sales of her clothes, as she doesn't have a bank account.

Without knowing it, the data that Maria publishes on her social networks is shared by the network with a credit analysis company, which uses it to define the credit score of individuals. This data includes information about her location, her interactions, the content of her posts and the comments she makes on other people's posts. The credit analysis company uses an algorithm that associates posts by people in economically vulnerable areas and mentions of financial difficulties with a low credit score. Maria, who already faces challenges because she doesn't have a formal credit history, ends up being disadvantaged by these associations. When she applies for a loan at a bank she has recently joined, Maria is surprised to be denied on the grounds that her credit score is insufficient for approval.

Even though her accounts are up to date and she has a promising business idea, Maria is penalized by the way her data has been interpreted together. To make the final decision, the bank added up aspects of her identity, such as the location recorded by her cell phone, her social media posts, the bank account that is linked to her cell phone, as well as other data such as that provided by Maria when she applied for the loan. The automated system did not take into account the totality of her financial reality, but only the biased data available in the digital infrastructure.

In order to guarantee autonomy, the structure of identity applications has been designed, including decentralized arrangements and self-sovereign identity models. In keeping with these premises, people have greater power over their own identity data and can share it selectively with other entities without depending on a central authority providing the identity and its validations.

The aim of this structure is to guarantee the user real control over their identity, increasing their **autonomy**. To this end, a self-sovereign identity must be able to transit and be validated, and it must allow the subject to choose when they want to disclose their data to a third party, what data they want to share, to which entity,

and for what purpose[24].

To realize these elements, **decentralized systems** generally use blockchain technologies, a type of *distributed ledger*, to enable the secure exchange of verifiable credentials. The *blockchain* essentially provides a decentralized domain not controlled by any individual entity. The data stored on any blockchain is readily available (availability property) to any authorized entity (access property)[25]. Given these characteristics, a decentralized identity structure would be linked to distributed registry tools.

In addition to decentralized systems, another tool considered to promote autonomy in DPI that uses identity solutions is the dissemination of mechanisms for **participation** in the development and implementation of the infrastructure and its applications. From the design of the DPI, so that the public value is delimited, to its implementation and monitoring, the active participation of different sectors of society is one of the keys to secure development that translates the common good.

This engagement is recognized by the Digital Government Strategy, since Decree No. 12.069 of 2024 determines joint work between the SGD and various other sectors to build a DPI. Through the engagement of various sectors, the relevance of innovation in the market and the provision of services to enhance people's experiences are highlighted.

It is only through the participation of groups of companies, civil society organizations, associations, consumers, researchers, academics and any other impacted agent that it will be possible to develop solutions centered on the citizen, the DPI user. Cooperation between actors enables the development of innovative solutions and the sustainability of the system[26]. By allowing other groups to actively contribute, governments can create a digital ecosystem that is more dynamic, sustainable and inclusive, as well as geared towards the needs of the society in

---

24 ALLEN, Christopher. The Path to Self-Sovereign Identity. 2016. Disponível em: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html. Acesso em: 28 jun. 2024.

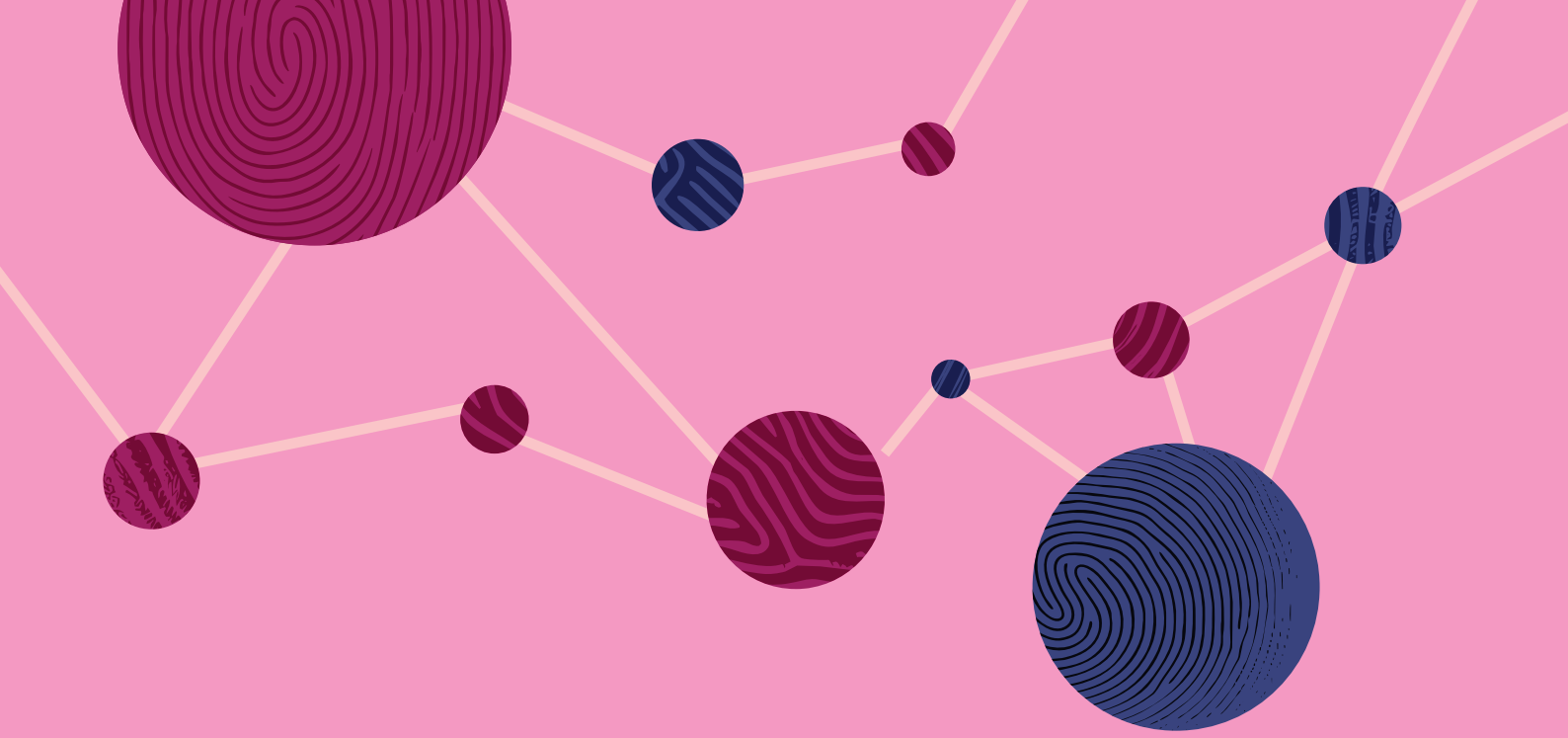
25 FERDOUS, Md Sadek; CHOWDHURY, Farida; ALASSAFI, Madini. In Search of Self-Sovereign Identity Leveraging Blockchain Technology. IEEE Access, v. 7, 2019. Disponível em: https://ieeexplore.ieee.org/document/8776589. Acesso em: 28 jun. 2024.

26 MASSALLY, Keyzom Ngodup, MATTHAN, Rahul, CHAUDHURI, Rudra. What is the DPI Approach? Carnegie Endowment for International Peace, 15 maio 2023. Disponível em: https://carnegieindia.org/2023/05/15/what-is-dpiapproach-pub-89721. Acesso em: 27 jan. 2024.

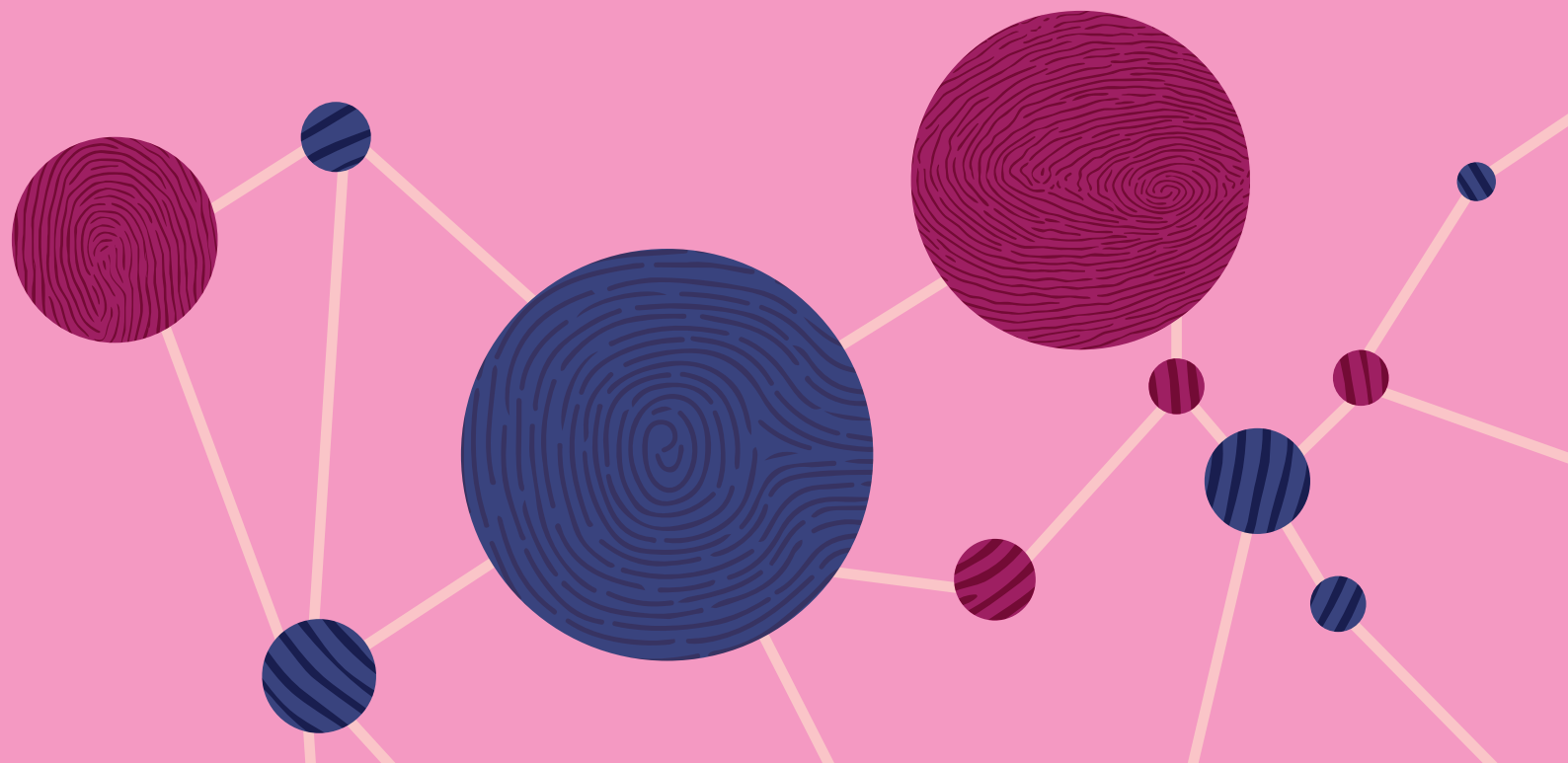
which the DPI is located.

The development of DPI brings various benefits and challenges that must be addressed in order to minimize the risks to people's rights in the face of the opportunities created by a digital infrastructure. It is in this context that this report will address how the DPI and identity ecosystem is perceived from the perspective of defending constitutional rights, especially the protection of personal data.

To this end, the Brazilian constitutional grammar of personal data protection will be analyzed, as well as the normative elements that make the right to data protection a reality, and the practices that guide the development of digital identity applications in a DPI. Based on the legal concepts established in Brazilian doctrine and case law, it is possible to identify concrete guidelines and directions for the implementation of digital identity applications at any level of a public infrastructure. These guidelines are fundamental to guaranteeing public value in digital identity, accountability in the use of personal data and effective participation in DPI.



02.
METHODOLOGY



2 Methodology

This report seeks to explore how the grammar of data protection, especially Brazilian constitutional jurisprudence, impacts on the development of identity applications in a DPI.

The hypothesis is that the grammar created by the right to the protection of personal data presents useful parameters to guarantee a fair flow of information, establishing, based on its principles, an information architecture design with adequate governance and *accountability* parameters.

To understand the extent of this hypothesis, this research looks at the grammar of data protection and DPI concepts in view of three complementary questions:

- The lack of articulation between the concepts of a digital identity, DPI and the grammar of data protection, especially in accordance with Brazilian constitutional jurisprudence;

- The risk of identity systems being designed in such a way as to reinforce and amplify historical injustices and asymmetries;

- The need to implement the normative parameters of personal data protection in DPI construction as part of its founding structure.

In light of this, this report seeks to understand the outlines of the following question: from a constitutional reading of the right to data protection, what governance measures should be implemented in a DPI context? To this end, fictitious cases are used to illustrate the tensions that exist in a DPI based on situations that are not real, but which bear some resemblance to reality and can therefore be implemented in the future.

We are experiencing a window of opportunity for the development of digital identity, given the dissemination of solutions such as Gov.br and the new National Identity Card (CIN). During the G20 presidency, Brazil experienced a geopolitical moment conducive to deepening issues related to DPI and the digitization of essential services. Furthermore, it is impossible to ignore the massive impact of digital identity solutions on people's daily lives, as they increasingly have to go through

identification and identity validation processes in the digital environment.

This document is the final report of the research project "Citizen Architectures in Digital Identity", in which Data Privacy Brasil sought to map the intersection between a digital identity and data protection in a DPI development context. For this reason, the methodology of this report is intertwined with the research development process itself.

The following activities guided the path of this research:

- ***Cards* for the general public:** in order to establish fundamental concepts about DPI and digital identity, cards were produced so that anyone, even those with little knowledge of the subjects, could understand and situate the debate initiated by the research. With the cards, it was possible to solidify the initial and basic concepts of the research project and publish accessible, low-complexity material.

- **Exploratory interviews:** fifteen exploratory interviews were conducted with experts from both the private and public sectors, academia and the third sector, to map out structures that are already being used to build a digital identity. The interviews were conducted by videoconference, were not recorded and were organized in a semi-structured way. This approach provided valuable insights into the challenges and opportunities at the intersection of DPI, data protection, data governance, transparency and access to a digital identity.

- **Event with experts:** work began on building the field and building bridges between public and private identity application development spaces, bringing together decision-makers, experts, civil society representatives and academics at the event "Common Horizons: the role of digital public infrastructure in finance, identity and climate justice" held on July 30, 2024 in Brasilia. At the event, Data was able to test the main points of questioning in a track dedicated to the theme of digital identity. The track was attended by professionals who split into smaller groups for discussions guided by questions produced by Data Privacy Brasil.

- **Review of national and international bibliography:** the concrete cases of digital identity that are already underway, the benefits that digital identity generates, the risks to fundamental rights, and possible recommendations for the development and expansion of a digital identity in line with the values of a DPI were analyzed. To this end, content cited in the interviews was analyzed, as well as other content produced by key players in the development of a DPI and digital identity applications.

- **UN public call for the report "Leveraging DPI for Safe and Inclusive Societies":** the United Nations Secretary-General for Technology (OSET) and the United Nations Development Program (UNDP) have published the report "Leveraging DPI for Safe and Inclusive Societies". Aapti and Data Privacy Brasil engaged in the process to provide feedback on the report and start a dialogue taking into account some contributions on data protection and human rights more broadly. On this occasion, it was identified that parameters were lacking to ensure meaningful multi-stakeholder participation throughout the DPI lifecycle. The final version of the report was published in DPI Safeguards.

- **Booklet "The infrastructure of identity: the influxes of a digital identity as an application of DPI":** the aim was to map and elaborate on the intersection of key concepts that would inevitably be used by agents working in the identity ecosystem. They would be able to recognize and apply the fundamentals, applications and functionalities of a digital identity in the context of DPI. In the booklet, Data Privacy Brasil began to draw its own interpretations of DPI and identity based on the organization's connections and parameters.

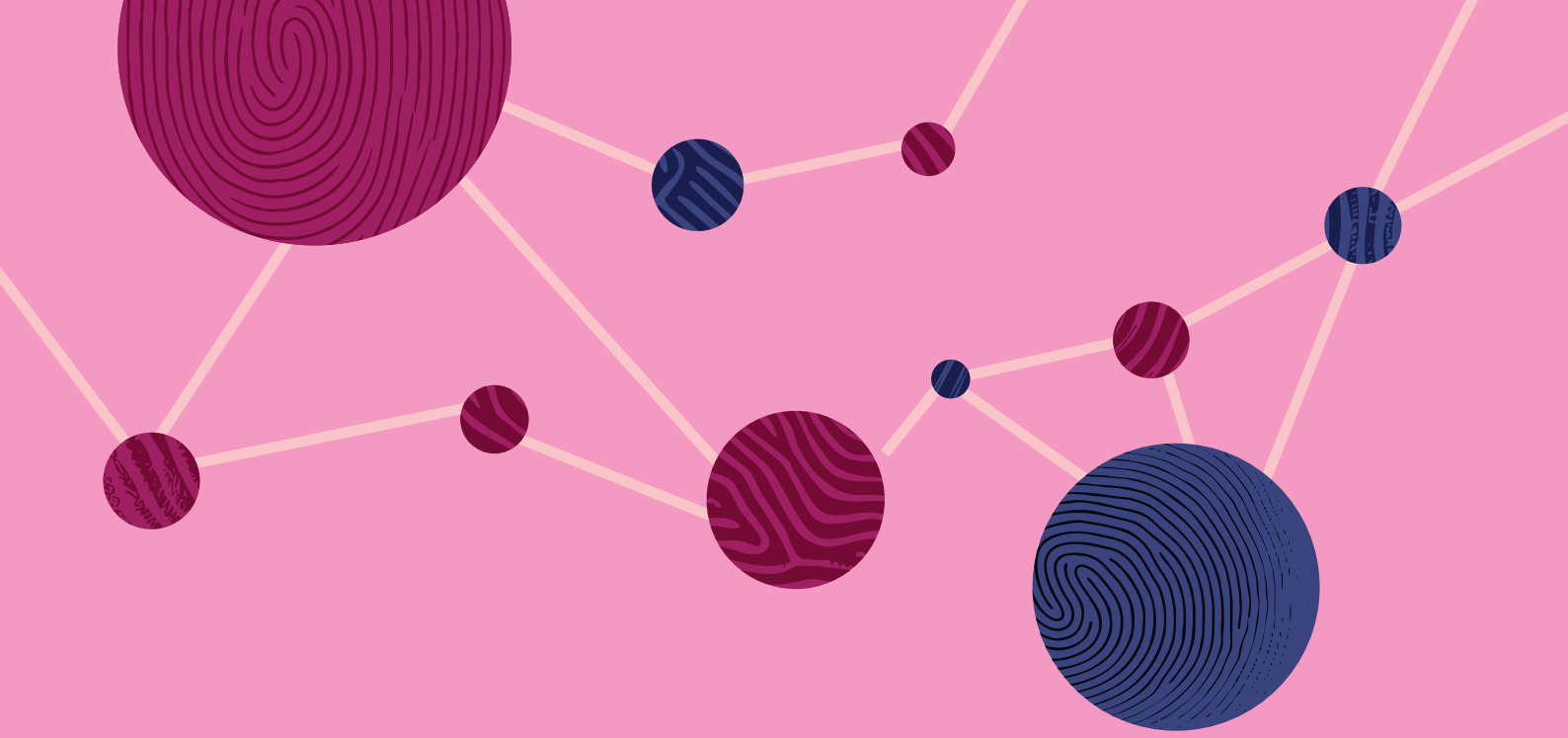
- **Episode of the Dadocracy podcast on the subject:** the episode sought to identify, from the interviewees' perceptions, the main challenges in the debate on identity and digital public infrastructure. To this end, the podcast featured interviews with Eduardo Lacerda, general coordinator of Civil Identification at the Digital Government Secretariat, Pedro Martins, academic coordinator at Data Privacy Brasil, Janaína Costa, a specialist in digital identity and independent consultant, and Yasodara Córdova, a specialist in digital identity and privacy at Único and part of the Co-Develop Fund investment board.

Based on these accumulations, this report was produced from a proactive approach to data protection, conceiving it not as a rule of secrecy, but as a component that fosters the fair flow of information by establishing procedures and parameters based on the promotion of fundamental rights.

By involving key stakeholders from the private and third sectors, public authorities and academia in the creation of a DPI, Data aims to directly influence the development of public policies in the field. The influence in this space is also the result of elaborations and deepening based on publications by other agents on the subject. This report is therefore divided into two main sections:

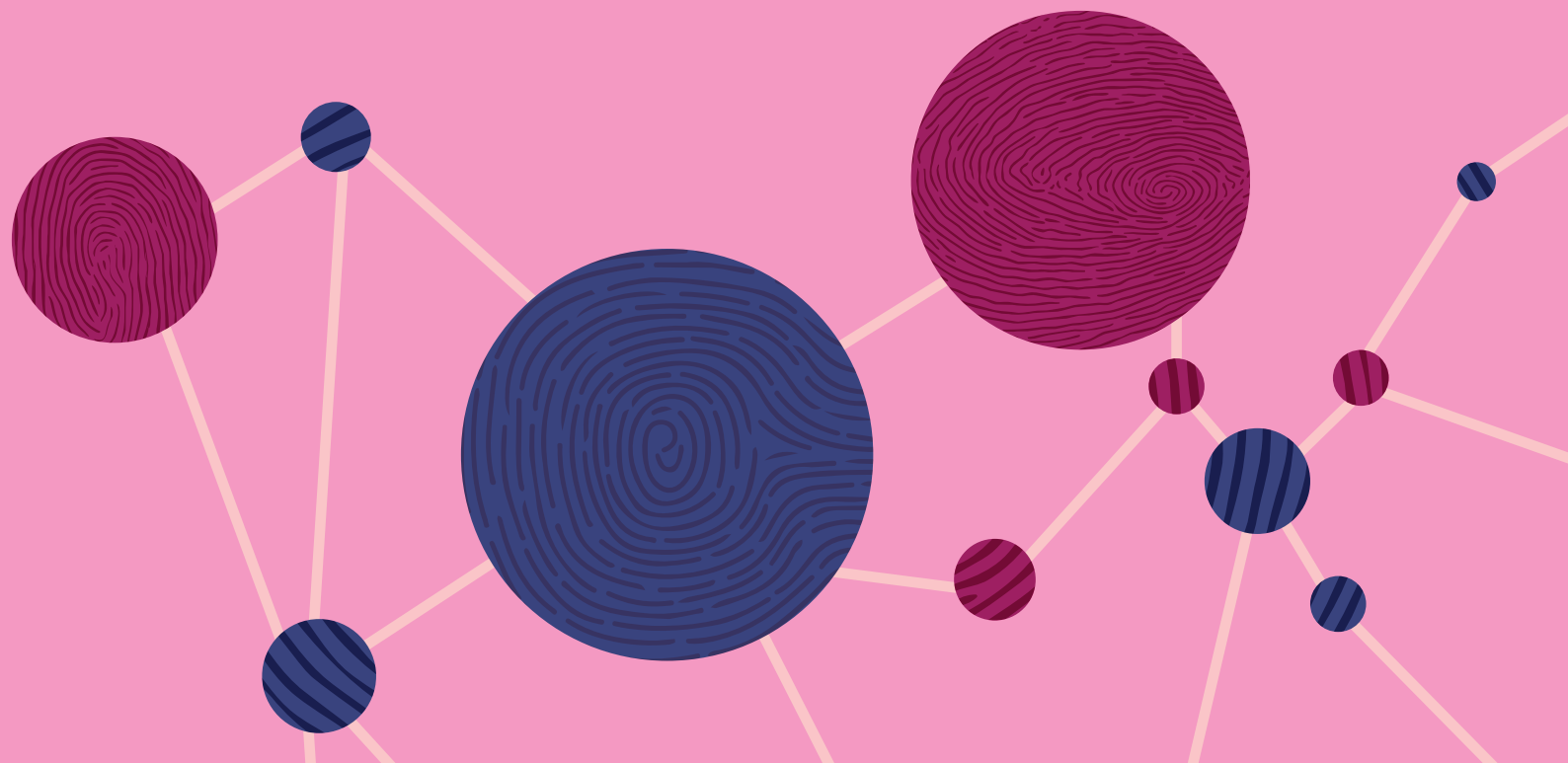
- The first deals with the grammar of data protection, with attention to Brazilian constitutional jurisprudence, which permeates concepts of privacy and data protection, privacy as contextual integrity and the informational separation of powers;

- The second section proposes ways of proceduralizing the rules in a DPI aimed at the common good from a constitutional reading of data protection on DPI applications, especially in guaranteeing a fair flow of information.



03.

BRAZILIAN CONSTITUTIONAL GRAMMAR ON DATA PROTECTION



3 Brazilian constitutional grammar on data protection

3.1. Privacy and Data Protection

The beginnings of discussions on the protection of personal data are rooted in the historical asymmetry of power between the state and the citizen, where the advancement of technology poses challenges to the right to privacy. The first generations of data protection laws emerged as a response to this power disparity, aiming to set clear limits on the collection and use of personal data by public authorities. With technological advances and increasing data processing, this asymmetry has intensified, and the understanding of fundamental rights has expanded, requiring new approaches and protection mechanisms.

In Brazil, the General Data Protection Law - Law 13.709/18 (LGPD) represents a regulatory response to ensure that the use of personal data takes place in line with the fundamental rights of privacy and data protection, establishing a new balance in the relationship between public authorities, private entities and citizens. The Federal Constitution (FC) itself, since its enactment, has determined a right to privacy as a fundamental right related to the protection of intimacy.

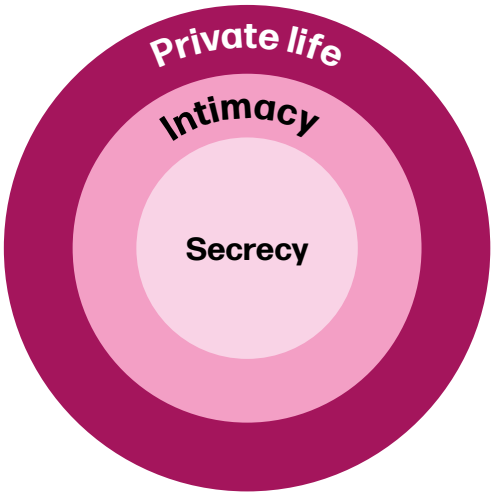
The right to privacy aims to protect the individual so that they can establish a space in which they "can develop their own personality, free from external interference"[27]. In a traditional sense, the right to privacy is associated with maintaining the secrecy of a private sphere of people's lives, which is opposed to the public sphere. This right to privacy is an **individual guarantee of non-intervention** by the state, in which the subject chooses not to make certain information about themselves available to other people, in other words, it is the possibility of the subject choosing to leave information about themselves out of the public domain[28] from the knowledge of third parties.

In this context, the scope of the right to privacy, provided for in Article 5, X, of the

27 DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Renovar: Rio de Janeiro, 2006, p. 96

28 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. São Paulo: Editora Gen, 2019, p. 95.

Federal Constitution, would be limited to guaranteeing that data from the **private sphere** does not circulate in other spheres without the owner having given cause to do so[29]. This narrower scope of protection is associated with the Hubmann doctrine, in which three concentric circles represent different degrees of manifestation of privacy, all subject to protection.



In this scheme, information known in the public sphere could not be protected by the right to privacy. This doctrine is in line with an interpretation that reinforces the dichotomy between personal information and public information, so that personal information could not be public and, if it were, it could not be protected as such.

However, with the advance of technology and forms of data processing, the scope of the right to privacy has been strained, even reinvented[30]. The debate on privacy increasingly touches on other concepts, which gain their own relevance, such as data protection and informational self-determination, for example.

The aim of this right is to guarantee that people have the autonomy to **develop their personality** and are not "subjected to forms of social control that would ultimately annul their individuality, curtail their private autonomy and make the free development of their personality unfeasible"[31]. This protection is based on positive action by the state, which creates regulations on the appropriate way to process

29 DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Renovar: Rio de Janeiro, 2006, p. 81

30 RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 15.

31 DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Renovar: Rio de Janeiro, 2006, p. 141-142.

data in compliance with people's rights.

Over time, data protection has gained relevance as a tool for **distributing power in society**[32]. It points to the incidence of principles and guidelines that should guide all data processing, especially guaranteeing transparency and publicity tools, specifying legitimate and non-abusive purposes, and data sharing rules, seeking to limit processing to the minimum necessary.

Based on the notion of data protection, the object of protection is no longer a group of data related to a subject's private life, but any data, including that which they share with other agents and which third parties exchange with each other. In this sense, identification data, such as name, CPF, affiliation, address, among others, even if they are disseminated on forms, collected by agents with no connection to the subject, or even made publicly available, are subject to legal protection. Furthermore, even data that does not uniquely identify the data subject but could lead to their identification, such as the location of the mobile device, habits and identification data on the internet, are subject to legal protection.

Faced with this framework presented by data protection, the Brazilian constitutional court was faced with debates precisely about the tension between privacy and data protection. In May 2022, the Federal Supreme Court (STF), in the judgment of Direct Action of Unconstitutionality (ADI) No. 6387, recognized **data protection as an autonomous fundamental right**. This action was aimed at declaring Provisional Measure (MP) 954/2020 unconstitutional[33]. EThis MP required all telephone operators to make available to the IBGE, in electronic form, the names, telephone numbers and addresses of millions of users of telecommunication services.

At the time, the intention was that this data could be used by the IBGE so that it could produce official statistics during the coronavirus public health emergency. The pandemic period prevented the IBGE from carrying out field research, due to social isolation, and the IBGE's justification was that, with the data processed by the telecommunications companies, it would be possible to reach citizens and carry out telephone interviews.

---

32 DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Renovar: Rio de Janeiro, 2006, p. 334.

33 PRESIDÊNCIA DA REPÚBLICA. Medida Provisória no 954, de 17 de abril de 2020. Planalto.gov.br. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv954.htm. Acesso em: 2 dez. 2024.

However, as early as the judgment on the precautionary measure, Justice Rosa Weber, the rapporteur, expressed concern about the MP's compliance with fundamental rights[34]. One of the greatest risks identified by the court was that of surveillance, in which the sharing of personal data carried out to achieve an initial purpose would end up being the basis for other processing activities that differed from that first purpose. This context was enough to draw the magistrates' attention to a possible misuse of data and the impact of sharing on citizens' rights.

In this sense, the plenary recognized that **there is no such thing as personal data without protection**, so that there is legal protection even for data that is not considered intimate or sensitive[35]. OIn other words, the right to data protection is different from the right to privacy precisely because it protects a different object[36] which is broader. With this, the STF recognized the emergence of a new right with a subjective and objective dimension, in which there are duties of protection on the part of the state to ensure that the subject maintains their sphere of individual freedom.

Following the judgment and in agreement with the court's position, the National Congress approved **Amendment to the Constitution No. 115/2022** to expressly provide for data protection as a fundamental right listed in art. 5 of the Federal Constitution. Thus, the protection of personal data, rather than a matter regulated by an infra-constitutional rule, has become a fundamental right of all people and, therefore, must be observed by all agents who are subject to the Federal Constitution, whether they are public bodies, companies or private organizations.

This means that the development of DPI solutions, including identity solutions, as they are services and activities intensely linked to the processing of personal data, also fall under the umbrella of activities that must comply with the constitutional right to data protection. Unlike traditional privacy, this right does not impose a barrier and conditions of secrecy or prohibition on data processing, but rather delim-

---

34 SUPREMO TRIBUNAL FEDERAL. Medida Cautelar na Ação Direta de Constitucionalidade 6.387 Distrito Federal. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15342959350&ext=.pdf. Acesso em: 2 dez. 2024.

35 SUPREMO TRIBUNAL FEDERAL. Referendo na Medida Cautelar na Ação Direta de Inconstitucionalidade 6.387 Distrito Federal. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15344949214&ext=.pdf. Acesso em: 2 dez. 2024.

36 MENDES, Laura Schertel. Decisão histórica do STF reconhece direito fundamental à proteção de dados pessoais. JOTA Jornalismo. Disponível em: https://www.jota.info/artigos/decisao-historica-do-stf-reconhece-direito-fundamental-a-protecao-de-dados-pessoais. Acesso em: 2 dez. 2024.

its concrete parameters so that the flow of data is appropriate to the principles of data protection, especially that of purpose, as will be analyzed in this document.

3.2. Personality development and autonomy

Associated with the fundamental right to data protection, another concept that is under strain due to the spread of DPI applications is that of **informational self-determination.** It was also cited by the STF's decision on Provisional Measure 954/2020 and is one of the foundations of the LGPD expressed in art. 2, II. The object of legal protection of self-determination is the free development of one's personality in accordance with one's subjectivity and autonomy.

As much as it is related to the idea of control, it is important to note that, like the right to data protection, self-determination is not limited to the decision-making process embodied in the data subject's consent. The authorization given by the data subject for a third party to process their personal data is not sufficient, adequate or the only way to guarantee that the data subject is exercising their self-determination, especially in contexts of a constant flow of personal data. Veridiana Alimonti specifies that the flow of data "does not necessarily depend on the individual's ability to control it from the outset. It refers to its compatibility with a broader protection discipline that establishes principles, limits and instruments that take into account the individual's perspective, but go beyond it"[37].

Thus, although "traditionally associated with the aspect of individual control over personal data, self-determination goes beyond the possibility of recognizing the data subject as a mere supplier of information about themselves and their context in return for access to goods, services, public policies and social benefits"[38]. The onus is not just on the data subject to authorize, consent to the processing of data, or even to share it with third parties; the object of self-determination goes beyond the data subject acting as the agent responsible for controlling their data.

---

37 ALIMONTI, Veridiana. Autodeterminação informativa na LGPD: antecedentes, influências e desafios. In: DONEDA, Danilo; MENDES, Laura Schertel; CUEVA, Ricardo Villas Bôas (coord.). Lei Geral de Proteção de Dados. A caminho da efetividade: contribuições para a implementação da LGPD. São Paulo: Thomson Reuters Brasil, 2020, p. RB-11.2.

38 ALMEIDA, Eduarda Costa. Diga-me os seus dados, que eu lhe direi quem você vai ser: o Direito à explicação como garantia da autodeterminação informativa na Lei Geral de Proteção de Dados Pessoais. 2023. 168 f., il. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade de Brasília, Brasília, 2023.

For Rodotà, "the possibility of control not only serves to assure citizens of the accuracy and correct use of information directly related to them, but can also become an instrument of balance in the new **distribution of power** that is taking shape"[39]. Self-determination justifies an effort that is not individual, "[r]ately the citizen is able to perceive the meaning that the collection of certain information can take on in complex organizations and endowed with sophisticated means for processing data, and the degree of dangerousness of the use of this data by such organizations may escape him"[40].

In a digital world, if informational self-determination is not protected, other rights such as the **free development of personality and autonomy** are compromised. This is because this foundation aims precisely to protect the ability of individuals to define for themselves what their interests and needs are and how they should be protected in a just society[41]. The widespread use of technologies jeopardizes precisely the ability of individuals or groups not to be bound by external constraints that they cannot overcome when they develop and discover their own preferences, characteristics, identities and interests.

This ability for people to determine themselves is "a precondition for a free and democratic communicational order"[42]. This is because, as a right of personality, it is through self-determination that a person has the tools to decide on the availability of their information to third parties and to develop their own personality, including the notion of the group, in order to interact in society and in public spaces, which are also being digitized.

This possible limitation of autonomy is linked to the definition of profiles based on the processing of personal data in different contexts, known as *profiling* practices. The aim of this practice is to ensure that, through the massive processing of data, it is possible to **predict and anticipate** events, such as human behavior and identity. The term "*data behaviorism*" translates precisely this process of produc-

---

39 RODOTÀ, Stefano. A vida na sociedade da vigilância. A privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 37.

40 RODOTÀ, Stefano. A vida na sociedade da vigilância. A privacidade hoje. Rio de Janeiro: Renovar, 2008, p. 37.

41 QUELLE, Claudia. Not just user control in the General Data Protection Regulation. On the problems with choice and paternalism, and on the point of data protection, Karlstad: Springer, 2017. In: LEHMANN, A.; et al. (orgs.). Privacy and Identity Management - Facing up to Next Steps. Karlstad: Springer, 2017.

42 SARLET, Ingo Wolfgang; SALES SARLET, Gabriele. Separação informacional de poderes no direito constitucional brasileiro. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022. p. 24

ing knowledge about preferences, attitudes, behaviors or future events without considering the psychological motivations, speeches or narratives of the subject, but based solely on data[43].

As a consequence, this process of *profiling* based on data affects the opportunities that are available to us and, consequently, the field of possibilities that defines us: not only what a person has already done or are doing, but also what he or she could have done or could do in the future[44].

Thus, in a context of data sharing and DPI, especially in relation to identity attribution and authentication structures, the potential for using correlations between this information opens a window for an exponential increase in the exchange, sharing, crossing and use of this data. This is because applications in DPI and other forms of technology are associated with a data flow scenario, precisely so that identity functions can be realized, but which must be fair from the point of view of structure and implementation.

At the same time as there is an intense flow of data, one of the effects of this process is the probabilistic logic of identification, in which it is no longer necessary or feasible to guarantee that a person has been properly identified. A margin of error is accepted which allows us to infer with a certain degree of certainty that a person corresponds to a certain profile or category. This logic, while useful in contexts of high data scale and speed of flow, such as the use of automated systems to prevent fraud or personalize services, can pose significant risks to fundamental rights. This is because people are determined based on assumptions about their behavior or characteristics that do not necessarily correspond to reality, but are derived from statistical correlations.

---

43 ROUVROY, Antoinette. The end(s) of critique : data-behaviourism vs. due-process. In: HILDEBRANDT, Mireille; DE-VRIES, Katja. Privacy, Due Process and the Computational Turn The philosophy of law meets the philosophy of technology. Oxon: Routledge, 2013. p. 143

44 ROUVROY, Antoinette. "Of Data and Men". Fundamental Rights and Freedoms in a World of Big Data. University of Namur, 2016. p. 22.

Hypothetical example

Identity as a probability

Isabela uses her credit card to make all her daily purchases. The bank where Isabela has an account and gives her the card collects metadata on financial transactions, such as the time of purchase, the frequency of purchases at the same establishment, the city region of the establishment, the value of the purchases, the sector of commerce, among other data. This information can be used by the bank to identify signs of fraud. If there is, and this signal is combined with various other indications, such as the consumer profile, the socio-economic profile of the cardholder, the place, time and value of the purchase, it is possible that the transaction will be identified as possible fraud, and Isabela will be identified from a characteristic attributed to her as a probable fraudster.

As much as the final attributed characteristic can be transmitted to other agents, so can the intermediate inferences, so that the inference made for a specific fraud detection context can be propagated through other spaces. In a DPI context, without the proper technical and governance safeguards, it is possible that the data collected on Isabela's credit card use, as well as data that indicates fraud, could be used for other purposes, such as increasing the value of the card insurance offered by an insurance company not linked to the bank responsible for the card or worsening the factors that indicate Isabela's likelihood of being considered a fraudster for access to a social assistance program.

With the digitalization, people are less and less able to fully exercise their **power of agency** over themselves. With the intense flow of data, data subjects lose visibility of who is processing their data and for what purposes. This prevents people from having the ability to self-identify and be authoritative in their individual or collective actions, since they are now identified on the basis of personal data they transmit, but also infra-individual and profile data that has been used to infer that characteristic.

Digital identity is not the transposition of an analog identity into the digital world. It

has its own nuances and meanings that go beyond biographical data and become the result of a sum of characteristics that flow through the digital infrastructure.

In this new context, there is a change in the logic of identification and subsequent validation. The previous logic was that the person would have a share of the power to reveal and know what information about them was being revealed, such as their full name, social security number, profile picture, address, etc. In addition, the person also knew and participated in the context in which that information would be used. With digitization and automation, the person loses their active role in the identification process, becoming an object to be identified by data they don't necessarily know and which is not exactly unique to them.

Hypothetical example

Controlling access to cultural events

Luciana wants to attend a concert at a large arena in her city. In the past, access control would have been simple: she would buy the ticket, present an identity document at the entrance (if necessary) and have her attendance confirmed via the physical or digital ticket. In this model, Luciana knew exactly what information was being revealed, such as her name, document number and a proof of purchase.

With digitalization, this process has been replaced by advanced facial recognition systems. When buying a ticket, the company selling the ticket asks Luciana to send a photo that will be used for identification at the entrance. On the day of the event, cameras installed in the arena capture images of all visitors, including Luciana, with automated systems analyzing facial features and checking them against the database of tickets sold.

In this model, Luciana has no control over what additional data may be collected beyond her facial image. For example, the system can associate her presence at the event with geolocation data, entry and exit times, or even cross-reference this information with other events she has attended in the past. In addition, the system can use analysis algorithms that identify behavioral patterns, such as gait or facial expressions, or to validate attendance using information that Luciana has not actively provided and may not even be aware is being used.

This process makes the person an object of identification, based on data they don't control and which may include statistical or correlational inferences that go beyond their original intention of just watching the show.

This new logic of identification is close to profiling practices, in which there is a notion of the person being identified by infra-individual data in order to form a supra-individual profile. Both processes position the person as an **object**, no longer a subject, in which the data and their profile are not necessarily representative of their self-declared identity. This "identity" is produced in aggregate form, from statistical data, in which the person loses the capacity for self-determination and becomes a profile in which it is possible to predict their interests and behavior

There is a change in the position of the identified person, from someone who reveals information to someone who has information revealed and associated with them. In the development of DPI and its identity applications, it is essential that there are mechanisms for subjectivation and claiming an identity in order to guarantee self-determination for the identified person and, with this, the exercise of the free development of their personality.

3.3. Contextual protection

In a scenario of *big data*, digitization and the development of digital public infrastructures, as well as the spread of data science, artificial intelligence, cross-checking and data mining tools, the impact of information processing on people's lives is significant.

Additional information

Right of access to information in the STF

In order to guarantee access to information and publicity of state acts, the government has made information and documents available on the internet for broad access by anyone interested. This has made the right of access to information more accessible than in the past, when data was handled physically, but it has also made it possible for other agents to access and process these documents and use them for other purposes. This availability of public records by the Judiciary is the subject of Extraordinary Appeal with Interlocutory Appeal 1307386, Theme 1141, which will be judged by the STF.

Given the high production and availability of personal data, especially in a DPI context, what types of protection and safeguards need to be developed in this scenario so that this flow of information has a positive impact on society? According to the **theory of privacy**[45] **as contextual integrity**[46], privacy protection is not about restricting access to personal data, making it secret, or assuming that the subject exercises control over their own information.

For this theory, privacy is preserved when the data flows generated comply with the **contextual information rules** applicable to that scenario. The assumption is that each sphere of life is governed by specific rules on appropriate information flows, such as the spheres in which a person acts as a mother, student and citizen, who in each sphere transmits specific information that is pertinent to that context. But what are these norms?

Contextual norms are those that establish expectations for characteristic behaviors depending on five elements[47]:

- **What is the data subject's social sphere?** Person to whom the data refers, whether a teacher, a candidate for political office, a child, a mother, a doctor, a consumer, a police officer, a friend, an elderly person, a debtor, a religious person, among others.

- **What is the social sphere of the sender?** Entity initiating the data flow, whether a telecommunications company, public welfare agency, public health agency, police station, financial institution, among others.

- **What is the recipient's social sphere?** Entity receiving the data flow, which may or may not be from the same group as the sending entity.

- What type of information? Personal data that is streamed, whether a per-

45 Nota-se que no contexto norte-americano, não há diferença expressa entre privacidade e proteção de dados, como apresentado no início deste capítulo. Nesse sentido, a ideia de privacidade contextual, como apresentado pela professora Nissenbaum, deve ser entendida como em linha com a perspectiva de proteção de dados brasileira, não apenas da privacidade em si.

46 Nissenbaum, Helen. Privacy in context: Technology, Policy and the Integrity of Social Life. Stanford: Stanford Law Books, 2010. p. 2

47 Nissenbaum, Helen. Contextual Integrity Up and Down the Data Food Chain, 20 Theoretical Inquiries L. 221 (2019). p. 229.

son's name, address, e-mail address, personal tastes, biometrics, affiliation, etc.

- **Are there any restrictions on streaming?** Impediments that the flow may have depending on other elements, such as consent or rules defined by law, resolution, practices, or contracts.

Thus, information flows are considered adequate to the extent that they conform to these norms, or at least do not violate them. All five elements must be taken into account in a flow conformity assessment, as they make up the contextual norm that indicates the feasibility of the flow taking place.

On the other hand, would an analysis of these five factors also resolve new situations in which there is no clear permission or restriction on transmission? If interpreted harshly, this theory would lead to a presumption that only data flows already consolidated by society would be favored. New ways of exchanging information could be seen as inadequate[48].

AThe theory indicates that, in addition to mapping these five elements, it is necessary to analyze the interests of the affected parties, political and ethical values, as well as contextual purposes and values, so that it is possible to see whether the data flow is suitable for privacy or not.

From the perspective of **interests**, ethical and political values, it becomes necessary to analyze elements such as who benefits and who is harmed by the treatment, how these people's interests and preferences are met, as well as identifying what the costs are and what the benefits are. These questions aim to understand whether there is a risk of identity theft, embarrassment, or an imbalance of power or diminished capacity to modulate their relationships or self-determination.

As for **contextual purposes and values**, the legitimate expectations of the data subject about the flow of information in the context in which it is processed must be taken into account. In this sense, it is important to stress that data traffic does not occur in a vacuum, but under a set of circumstances that guide the integrity

48 BIRNHACK, Michael D. A quest for a theory of privacy: context and control. Disponível em http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1824533. Acesso em 08 set. 2024. p. 21.

of the flow[49]. Thus, even after considering the five parameters on the adequacy of the data flow, the **legitimacy** of the flow must be analyzed based on the interests, social values and contextual purposes and values of the processing that initiated the flow. This is because the premise of contextual privacy is to confront the processing of personal data in which there is a significant gap between a contextual expectation and the practice of the agent processing the data.

Hypothetical example

Health data flow

Joana is seeking medical help to investigate symptoms of a foodborne infection after eating at a large restaurant chain in her city. To do so, she made an appointment with the doctor at her neighborhood health center, scheduled through the Union's health platform.

The doctor asked Joana to carry out a series of tests at a partner clinic and to return as soon as the results had been obtained. Joana carried out the tests at a clinic that has a service for sending the results to the doctors requesting the test, but the patient did not authorize direct sharing and preferred to collect the results herself. On her return visit, Joana presented the results to the doctor, who confirmed the food poisoning.

The patient, who was careful about sharing her data, asked the doctor for the tests after her diagnosis. Despite her request, the test results were sent to the body responsible for health surveillance so that the restaurant that caused Joana's diagnosis could be inspected and so that the spread of the disease could be contained. Thus, given that the treatment was appropriate and that there was no need to collect the data subject's consent, the context of the treatment allowed the flow of Joana's data between the doctor and the health agency to serve a purpose that went beyond the data subject's interests, but which was close to her expectations in the patient-doctor relationship.

49 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 216

From a contextual integrity reading of privacy, it is possible for the right to data protection to be an instrument for people to develop their personality freely. The availability of data does not indicate an unrestricted flow of data that ignores the circumstances of the processing, but neither does it prevent any transit of data in the name of a logic that the data subject should control any exchange of data about them.

The information flow has fundamental value for the entities that make it up to play their expected social roles[50]. It is from these perspectives, whether mapping the five elements or observing the ethical and contextual interests and values of the case, that the **information flow** must be understood as **integral**. These ethical and contextual parameters provide the necessary flexibility in a scenario of constant change and the digitalization of life, in which various elements of life are now in the digital world.

Also according to the theory of privacy as contextual integrity, the definition of these contextual expectations of data subjects is also related to elements of **transparency**, **accountability** and burden of proof[51]. This is because the data subject is not surprised when they know the flow in which they are inserted and have aligned their contextual values. With this information, the data subject, as well as society as a whole, will have the necessary tools to question and hold accountable those processing agents who carry out certain stages of the flow inappropriately.

The flow of personal data in a DPI must be analyzed from a contextual privacy perspective in order to ensure that the exchange of information complies with privacy values and, more specifically, with the fundamental right to the protection of personal data. Under this approach, the law does not aim to put up barriers or halt the flow of personal data; this transit of information is guided by specific regulatory considerations according to the **contextual relationship** established between the agents affected by the flow.

Based on this theory, the integrity of data traffic is perceived according to the con-

50 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019. p. 216

51 NISSENBAUM, Helen. Contextual Integrity Up and Down the Data Food Chain, 20 Theoretical Inquiries L. 221 (2019). p. 256.

text in which the flow itself is inserted[52]. If there are doubts about **who the agents are and what information makes up the flow, and about the ethical and contextual values that are promoted or obscured** by the processing[53], the flow is no longer perceived as intact and must be re-evaluated. This is why data sharing, including identity data in an infrastructure, can take place as long as it observes the context in which it is inserted.

3.4. Information separation

The digitalization of life also affects the way in which information is structured, organized and made available to the agents that make up this digital space. For this reason, in addition to the context in which this data was collected, the concept of informational separation is another key to reading the constitutional right to data protection.

Informational separation has its origins in the concept of informational separation of powers and, consequently, in the theory of separation of powers. The aim of this theory is to **divide political power** into different people in order to prevent the concentration of this power[54]. This division of powers is related to the principle of the division of tasks in the state, in which the state bodies that make up the state have their own functions and **competencies** and can exercise them with relative autonomy, without interference or dependence on others[55]. At the same time as there is a division of powers in limited spheres of competence, the powers act jointly to achieve common constitutional objectives[56].

In the light of **digital constitutionalism**, these classic principles have been reframed in the context of digitalization, including of the state, in which an informa-

---

52 BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento.Rio de Janeiro: Forense, 2019. p. 212.

53 RODRIGUES, Amaury de Matos. A controvérsia sobre a divulgação de remuneração dos servidores públicos: uma análise à luz da privacidade como integridade contextual. Dissertação (mestrado) – Instituto Brasiliense de Direito Público – IDP, Brasília, 2014. p. 60.

54 MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet. Curso de Direito Constitucional, 7ª Ed. São Paulo, Saraiva, 2012.

55 SILVA, Virgílio Afonso da. Direito Constitucional Brasileiro. São Paulo: Editora da Universidade de São Paulo, 2021. p. 33

56 SARLET, Ingo Wolfgang; SALES SARLET, Gabriele. Separação informacional de poderes no direito constitucional brasileiro. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022. p. 28

tional separation of powers must be guaranteed. In other words, the state should not be understood as an **informational unit** in which all its bodies have the same data at their disposal, as the state is organized in powers, in competences, which should limit even the information that its bodies can access.

As a result, the flow and sharing of personal data between state bodies must comply with the competencies, functions and powers of the agents involved in this ecosystem. Furthermore, the data processing carried out by an entity must be in accordance with its competences, at the risk of enabling a **concentration of power.**

This concept has been debated by the STF in several decisions issued by the court, three of which are worth highlighting.

ADI nº 6529/DF - Abin case

In October 2021, the full STF handed down judgment in **ADI No. 6529/DF** and ruled that the sole paragraph of art. 4 of Law No. 9.883/1999 was constitutional, with a conforming interpretation[57]. This provision allows the Brazilian Intelligence System (SISBIN) to share data related to the defense of national institutions and interests with the Brazilian Intelligence Agency (Abin).

For the ADI plaintiffs, this legal permission was not in line with the maintenance of fundamental rights and guarantees, with international agreements, even with Brazilian norms. The law that is the subject of the action would be in opposition to the rules that provided for a duty of motivation, reasonableness and proportionality in the sharing of information, as well as duties of secrecy recorded by reservation of jurisdiction. This is because, according to the plaintiffs, "there has recently been a gradual increase in Abin's power to request information" and "the possibility of distorting Abin's purpose cannot be ignored".

The entire dispute was based on whether or not SISBIN could provide data to Abin without the proper constitutional guidelines. In this sense, the STF affirmed that, despite the secretive nature of the intelligence activities carried out by Abin, they cannot be removed from the external control of the Legislative Power (Article 49, X, of the Constitution) and the Judiciary Power (Article 5, XXXV, of the Constitution) in

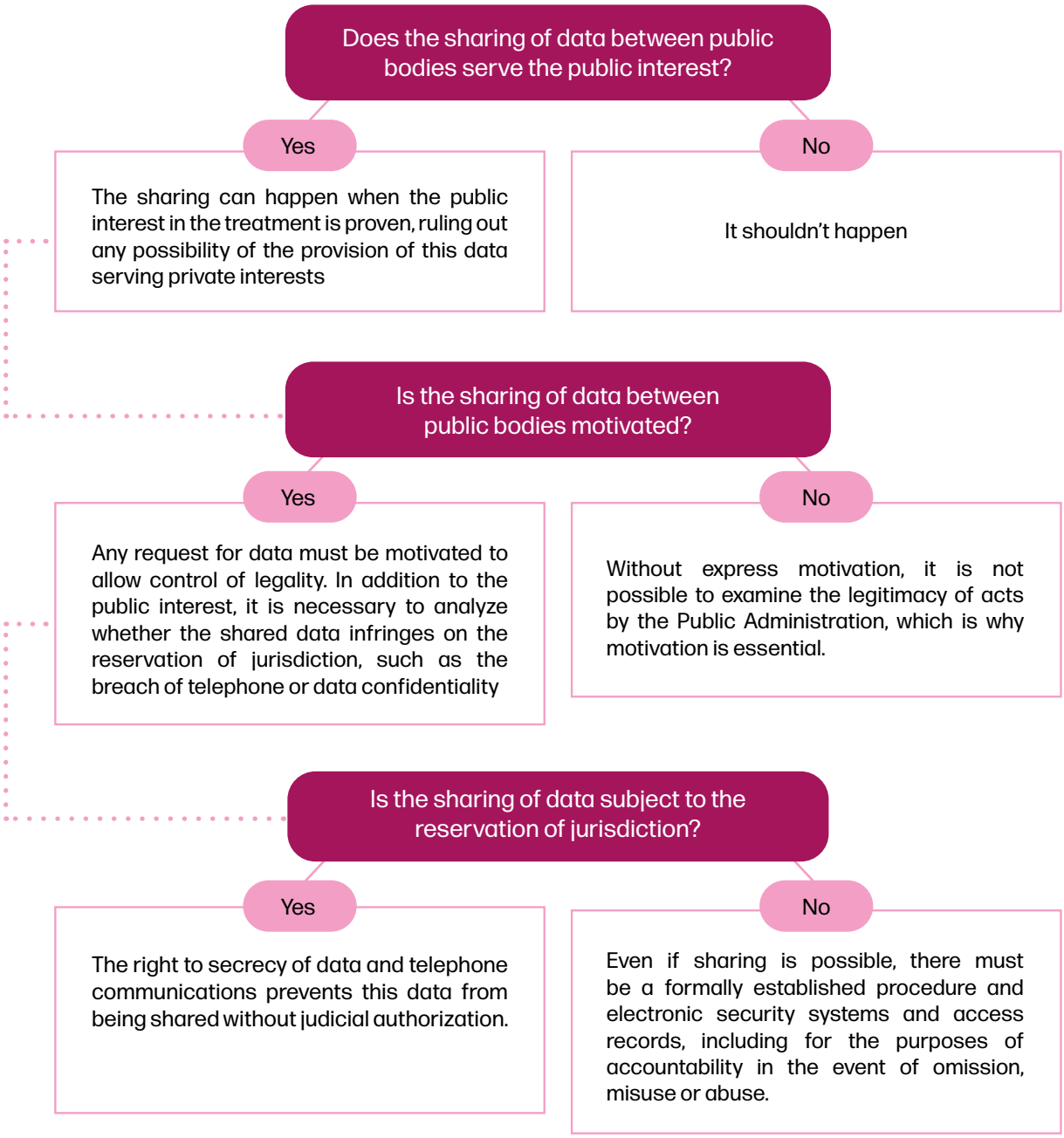
57 https://portal.stf.jus.br/processos/downloadPeca.asp?id=15348384228&ext=.pdf

order to verify the strict public purposes to which the data processing is directed.

Thus, the court ruled that the provision of information between bodies that does not comply with the formal rigors of the law or strictly serve the public interest, legally labeled as the defense of institutions and the national interest, constitutes an abuse of the right, contrary to the legitimate purpose set out in the legal norm.

Against this backdrop, the STF argues that the sharing of data, whether personal or not, must serve a specific and public purpose, i.e. if the body receiving the data does not have a reason for doing so, it should not be processed. There is a separation of competences between public bodies, which must also be respected at an informational level, so that only the relevant authorities should process certain data.

Based on the STF's decision, the following infographic can be made:


Does the sharing of data between public bodies serve the public interest?
Yes
The sharing can happen when the public interest in the treatment is proven, ruling out any possibility of the provision of this data serving private interests
No
It shouldn't happen
Is the sharing of data between public bodies motivated?
Yes
Any request for data must be motivated to allow control of legality. In addition to the public interest, it is necessary to analyze whether the shared data infringes on the reservation of jurisdiction, such as the breach of telephone or data confidentiality
No
Without express motivation, it is not possible to examine the legitimacy of acts by the Public Administration, which is why motivation is essential.
Is the sharing of data subject to the reservation of jurisdiction?
Yes
The right to secrecy of data and telephone communications prevents this data from being shared without judicial authorization.
No
Even if sharing is possible, there must be a formally established procedure and electronic security systems and access records, including for the purposes of accountability in the event of omission, misuse or abuse.

This ruling does not make any sharing of data between government bodies rigid. It can take place as long as there is:

- observance of the public interest;
- motivation of administrative acts;
- analysis of the need for secrecy and reservation of jurisdiction.

In this sense, the rapporteur, Cármen Lúcia, states that the possibility of providing information is in line with cooperative federalism and does not constitute an invasion of political autonomy. Thus, when these requirements are met, data can and should flow between public agents.

ADI nº 6649/DF and ADPF nº 695/DF - Citizen's Base Register Case

In September 2022, the STF had the opportunity to judge a similar case in **ADI No. 6649/DF and in the Argument for Non-Compliance with a Fundamental Precept (ADPF) No. 695/DF**, in which the constitutionality of Decree No. 10,046/2022 was questioned[58].

Decree No. 10.046/2019 provides for governance in data sharing within the federal public administration, and establishes the Citizen Base Register (CBC) and the Central Data Governance Committee[59]. The aim of the Decree was to facilitate the process of sharing data, including personal data, between entities of the direct, autonomous and foundational federal public administration and the other branches of the Federal Government. According to Article 1 of the Decree, its purpose was to simplify the provision of public services, optimize the formulation and monitoring of public policies, and promote the quality of data held by federal agencies.

To this end, art. 5 of the Decree determined that it would not be necessary to enter into an agreement, technical cooperation agreement or similar instruments in order to share data between the bodies governed by the Decree.

As soon as it was published, the Decree was used to justify the sharing of per-

58 SUPREMO TRIBUNAL FEDERAL. Ação Direta de Inconstitucionalidade 6.649 Distrito Federal. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978491&ext=.pdf. Acesso em: 2 dez. 2024.

59 PRESIDÊNCIA DA REPÚBLICA. Decreto n 10.046, de 9 de outubro de 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d10046.htm. Acesso em: 2 dez. 2024.

sonal data from the National Driver's License, managed by the National Traffic Secretariat (Senatran), formerly Denatran, between the Federal Data Processing Service (Serpro) and Abin. This was one of the facts that prompted the ADPF in question to be filed. As a result of the legalization of the case, Denatran revoked the Term of Authorization that allowed the sharing of data with Abin. Even with the possible loss of purpose of the ADPF, Justice Gilmar Mendes, the rapporteur, upheld the judgment, considering that the act of the Public Power challenged in this ADPF covered an entire framework of legal insecurity generated by distorted interpretations of Decree 10.046/2019[60].

The rapporteur's vote, which was the guiding vote of the judgment, gave a conforming interpretation to the Decree in order to present guiding parameters for data sharing.

For the STF, if, on the one hand, the signing of agreements and technical cooperation agreements could be a barrier to sharing, one of their purposes was precisely to guarantee the publicity of the sharing. The court reinforced the government's commitment to transparency about the sharing it carries out, as it is the government's duty to give due publicity to the cases in which each government entity shares or has access to personal databases[61].

The Supreme Court ruled that data sharing between public administration bodies and entities can only take place when it is publicized and upfront:

- the choice of legitimate, specific and explicit purposes for the processing of data (art. 6, I, Law 13.709/2018);
- the compatibility of the processing with the stated purposes (art. 6, II);
- the limitation of sharing to the minimum necessary to fulfill the stated purpose (art. 6, III);

60 SUPREMO TRIBUNAL FEDERAL. Arguição de Descumprimento de Preceito Fundamental 695 Distrito Federal. p. 5. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978671&ext=.pdf. Acesso em: 29 jul. 2024.

61 SUPREMO TRIBUNAL FEDERAL. Arguição de Descumprimento de Preceito Fundamental 695 Distrito Federal. p. 3. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978671&ext=.pdf. Acesso em: 29 jul. 2024.

- full compliance with the requirements, guarantees and procedures established in the General Data Protection Law, insofar as it is compatible with the public sector.

These requirements are very similar to those of the court's decision in ADI 6529/DF. On the one hand, in this ADI, the data sharing requirements are based on the concepts of public interest and misuse of purpose defined in the constitution itself. On the other hand, in ADI 6649/DF, the dialog with the provisions of the LGPD are expressed, in order to complement the elements brought by the constitution. According to both judgments, the sharing of data must comply with requirements common to data protection for the analysis of the constitutionality of the sharing of personal information, making explicit the dialog between the subjects.

In the ADI in question, the STF explicitly reinforces the understanding of ADI 6529, and takes up arguments in line with the principle of the informational separation of powers. As a summary of the two judgments, for the court, this type of sharing must comply:

- the adoption of measures that are proportionate and strictly necessary to serve the public interest;

- the establishment of a formal administrative procedure, accompanied by prior and exhaustive motivation, to allow the Judiciary to control its legality;

- the use of electronic security and access registration systems, including for accountability purposes in the event of abuse; and

- compliance with the general principles of protection and the rights of the data subject provided for in the LGPD, insofar as this is compatible with the exercise of this state function.

It is worth noting that the public interest should not be analyzed as a superior legal good and in confrontation with other constitutional values, such as data protection and privacy. This is because, if privacy is analyzed as an individual interest, it would succumb to the collective interest, in which the Government could process data in an unrestricted manner for public purposes, which are considered superi-

or[62]. Thus, data protection must be understood as a tool for achieving the collective goals of structuring democratic regimes, while at the same time guaranteeing people's autonomy[63].

Another fundamental element considered by the STF's final decision was the composition of the Central Data Governance Committee provided for in the Decree. This composition was deemed unconstitutional by the court because it was made up only of representatives of the federal public administration, but should have had an "independent, plural composition open to the effective participation of representatives of other democratic institutions".

The Committee would be responsible for setting limits on data sharing between federal public administration bodies, a fact that has cross-cutting effects on public sector activities. For this reason, the STF recognizes the need for it to be representative and to demonstrate an openness to pluralizing the debate beyond representatives of the public authorities in order to guarantee the effectiveness of the fundamental right. **Civic participation**, as recognized by the STF, is **a central tool for legitimizing the activities carried out by the state**, which is why it will be the subject of more specific analysis in the following chapter.

MS nº 36.150/DF - INEP x TCU case

Finally, in December 2021, the STF ruled on **Writ of Mandamus (MS) No. 36.150/DF**, on the possibility of sharing personal data between government bodies[64]. The MS was filed by the Anísio Teixeira National Institute for Educational Studies and Research (INEP) against a ruling by the Federal Court of Auditors (TCU) that determined that individualized data from the School Census and ENEM should be handed over for an audit of the Bolsa Família Program.

For INEP, sharing information with the TCU for external control would be contrary to the expectations of the students who provide their data, jeopardizing INEP's

62 BLACK, Gillian e STEVENS, Leslie. "Enhancing Data Protection and Data Processing in the Public Sector: The Critical Role of Proportionality and the Public Interest" . In: Scripted. Vol. 10, n. 1, 2013, p. 95.

63 SUPREMO TRIBUNAL FEDERAL. Ação Direta de Inconstitucionalidade 6.649 Distrito Federal. p. 33. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978491&ext=.pdf. Acesso em: 2 dez. 2024

64 SUPREMO TRIBUNAL FEDERAL. Mandado de Segurança 36.150 Distrito Federal. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15349322719&ext=.pdf. Acesso em: 2 dez. 2024.

ability to conduct research and monitor public education policies, and would infringe on the rights of third parties who are guaranteed confidentiality of their personal data. The TCU, on the other hand, claims that item 16.3 of the ENEM 2017 Public Notice allows the use of personal information within the scope of government programs and that its auditors are empowered by law to access personal information, even if it is confidential.

On the one hand, the STF recognizes the confidential nature of the data processed by INEP, on the other hand, the TCU has the power to carry out audits and the attribution of this power presupposes the recognition of the means necessary to fulfill this duty. For this reason, the controversial question is whether the duty of secrecy imposed on INEP would be breached by transmitting these individualized databases from the Educational Census and ENEM to the TCU. This analysis of the competence of public bodies is directly linked to the debate on the informational separation of powers, so that the body could and should access all the data necessary to carry out its duties.

In his vote, still on the precautionary measure of the MS, Justice Barroso believes that the sharing of personal data to another public body for a purpose other than that initially declared subverts the authorization of those who provided their personal data, in apparent violation of the duty of secrecy and the guarantee of inviolability of intimacy[65]. Thus, the sharing of data would undermine students' trust in INEP, which could violate the statistical confidentiality between INEP and the students and could jeopardize the continuity of the activities carried out by INEP itself.

In this judgment, Justice Barroso expressly takes up the court's decision in ADI 6649 and ADPF 695 in view of the impact of the data-sharing regime between public bodies on the protection of fundamental rights.

From an analysis of the three cases in question, the STF's position on the need to temper the sharing of data between government bodies, justified by the **efficiency** and **digitalization** of the administration, with **constitutional values** that indicate the delimitation of a **specific and compatible purpose** for the processing, in addition to the public interest and imbricated **publicity**, is evident.

---

65 SUPREMO TRIBUNAL FEDERAL. Medida Cautelar em Mandado de Segurança 36.150 Distrito Federal. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15339236967&ext=.pdf. Acesso em: 2 dez. 2024.

This care with the purpose of data sharing is directly in line with the principle of the informational separation of powers.

This separation of personal information that can be processed is justified by the idea of a functional division of competence and attributions so that **limits can** be set on **the exercise of political power**. In the digital context, this means that the state must establish, through the use of parameters for action forged on the basis of the principle of separation of powers, an organizational regime based on the division of competences, making every effort to avoid the abusive, disproportionate, unrestricted and therefore unconstitutional sharing of personal data.[66]

Thus, the STF's judgments point to the well-established interpretation that the state is not one, even when it comes to the personal information it establishes and knows. Following the logic of the separation of powers, the division of competences defined in the constitution should also guide the form and parameters of the sharing of personal data. At the very least, this data cannot be shared unrestrictedly by the entities that make up the Public Power, especially when there is no purpose for it or it is different, under penalty of misuse of purpose.[67]

One way of avoiding possible abuses in data sharing is to guide the flow of data by **dividing up the powers** of the agents who send and receive personal data. This separation of competences, of powers, of public bodies is directly related to identifying the specific purposes of the processing that certain agents carry out on the basis of their competence[68]. This assessment of the parameters for data sharing indicated by the STF is complementary to the one already presented by the ANPD in its Guidelines for the Processing of Personal Data by the Public Authorities[69]. The parameters of the two sources can be compared as follows:

---

66 SARLET, Ingo Wolfgang; SALES SARLET, Gabriele. Separação informacional de poderes no direito constitucional brasileiro. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022.

67 SARLET, Ingo Wolfgang; SALES SARLET, Gabriele. Separação informacional de poderes no direito constitucional brasileiro. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022.

68 SARLET, Ingo Wolfgang; SALES SARLET, Gabriele. Separação informacional de poderes no direito constitucional brasileiro. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022. p. 34.

69 ANPD. Guia Orientativo de Tratamento de dados pessoais pelo Poder Público. 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 20 dez. 2024.

STF	ANPD[70]
Full compliance with the requirements, guarantees and procedures established in the LGPD, insofar as it is compatible with the public sector.	Documentation of the treatment operation by means of a technical and legal analysis governing sharing.
Establishment of a formal administrative procedure, accompanied by prior and exhaustive motivation, to allow the Judiciary to control its legality.	Formalization of the treatment operation by signing a contract, agreement or similar instrument.
Assessment of the compatibility of data sharing, verifying whether the sharing of personal data to another public body for a purpose other than that initially declared undermines the authorization of the data subjects.	Identification of the personal data being shared and the specific purpose of the data being processed, verifying the compatibility between the original purpose and the purpose of the sharing.
Full compliance with the requirements, guarantees and procedures established in the LGPD, insofar as it is compatible with the public sector.	Assignment of an appropriate legal basis for the sharing activity, as well as the initial and final term of the processing.
Obligation of the public body to give due publicity to the cases in which each government entity shares or has access to personal databases.	Information, in a clear and accessible manner, to the data subject about the sharing and the means to exercise their rights.
Use of electronic security systems and access logs, including for accountability purposes in the event of abuse.	Adoption of information prevention and security measures, including technical and administrative measures to protect personal data from security incidents.
Full compliance with the requirements, guarantees and procedures established in the LGPD, insofar as it is compatible with the public sector.	If necessary, the adoption of additional measures, such as the preparation of a data protection impact report, definition of the financial burden of data sharing and the possibility of further sharing or transfer.
Adoption of measures that are proportionate and strictly necessary to serve the public interest.	Assessment of the compatibility between the original purpose and that of the secondary use, taking into account the public interest and the specific public purpose of the subsequent processing, as well as its link to the legal competencies of the bodies or entities involved.

70 MARTINS, Pedro Bastos Lobo; SANTOS, Pedro Henrique; CRUZ, Sinhue Nascimento. Guia ANPD: Tratamento de Dados pelo Poder Público. 2022. Data Privacy Brasil.

In addition to the first moment in which the controller collects personal data from the data subject, the LGPD presents some tools to be used by processing agents when they do not have direct contact with the data subject, or in data reuse scenarios. Any processing of data must take place in order to achieve legitimate, specific, explicit and informed purposes, without the possibility of further processing incompatible with those purposes[71].

It is quite common that in cases of intense data sharing and flow, common to DPI scenarios, the information processing architecture is complex and, in addition to the subject, the information is **validated** on the basis of other agents. This is very evident in identity applications, especially in authentication and authorization functions, where the validity of the information presented by the subject is confirmed with other agents, including the credential issuer. In this verification process, data processed by private or public entities can be consulted in different contexts.

In the context of the informational separation of powers, state intervention cannot compromise the objective or the public purpose that gave rise to the processing, justifying the collection of personal data under penalty of misuse of purpose[72]. he sharing of data guarantees the importance of the duty of transparency, from the moment of collection, of the processing agent towards the data subject, since it is an objective condition for the exercise of rights such as the right to object to new processing[73]. Thus, the use of data for **secondary purposes** depends on:

- indication of an appropriate legal basis to support the new treatment;
- compatibility of the secondary purpose with the purpose of data processing at the time of data collection, the primary purpose;
- the provision of a sufficiently specified purpose, which allows the assessment of the public interest to be achieved;

---

71 PRESIDÊNCIA DA REPÚBLICA. Lei n 13.709, de 14 de agosto de 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 2 dez. 2024.

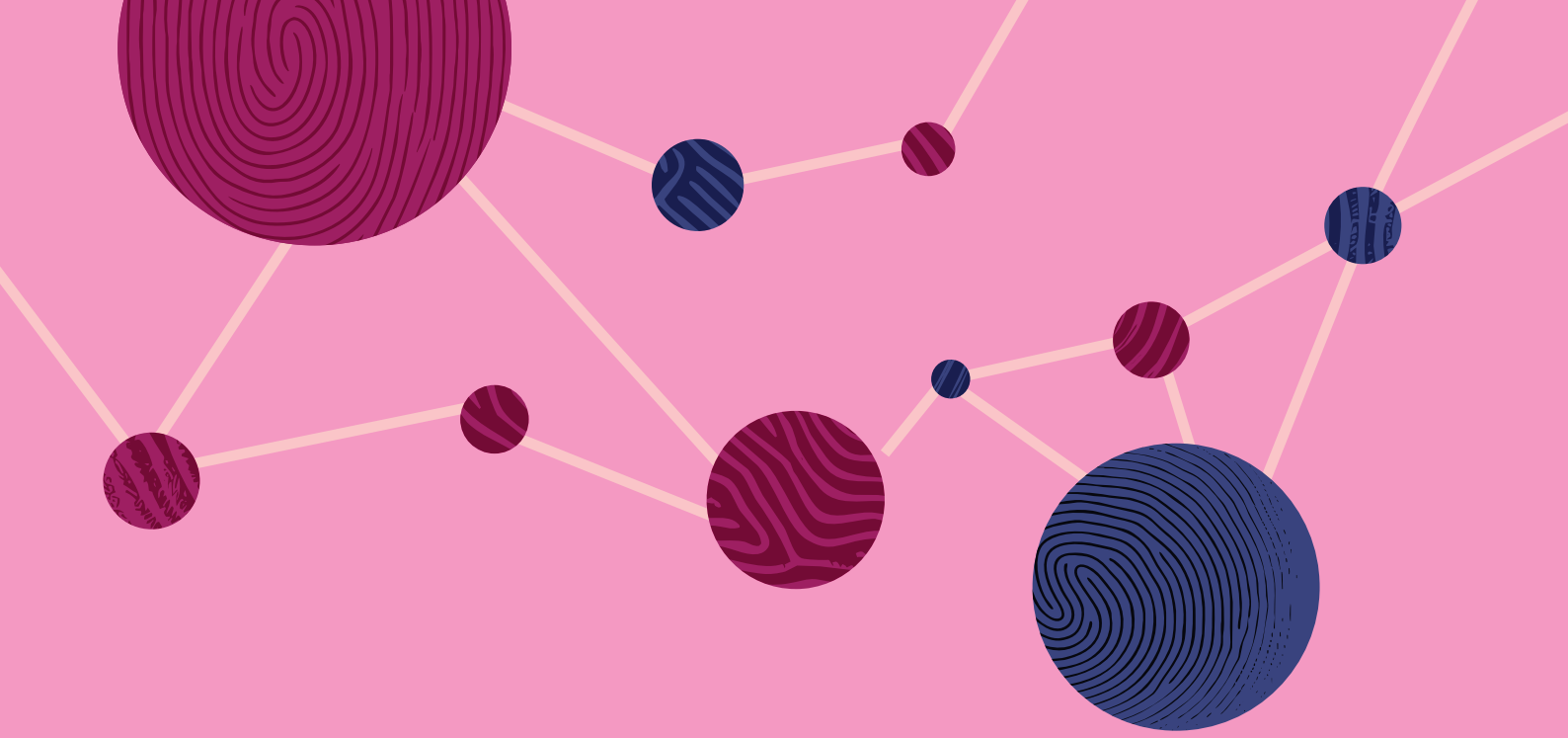
72 SARLET, Ingo Wolfgang; SALES SARLET, Gabriele. Separação informacional de poderes no direito constitucional brasileiro. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022. p. 34.

73 WIMMER, Miriam. Limites e possibilidades para o uso secundário de dados pessoais no poder público: lições da pandemia. Revista Brasileira de Políticas Públicas, Brasília, v. 11, n. 1. p.122-142, 2021. p. 137.

- compliance with the principles of data protection and the rights of data subjects, in particular the principle of transparency, necessity, adequacy and accountability and the right to information and access.

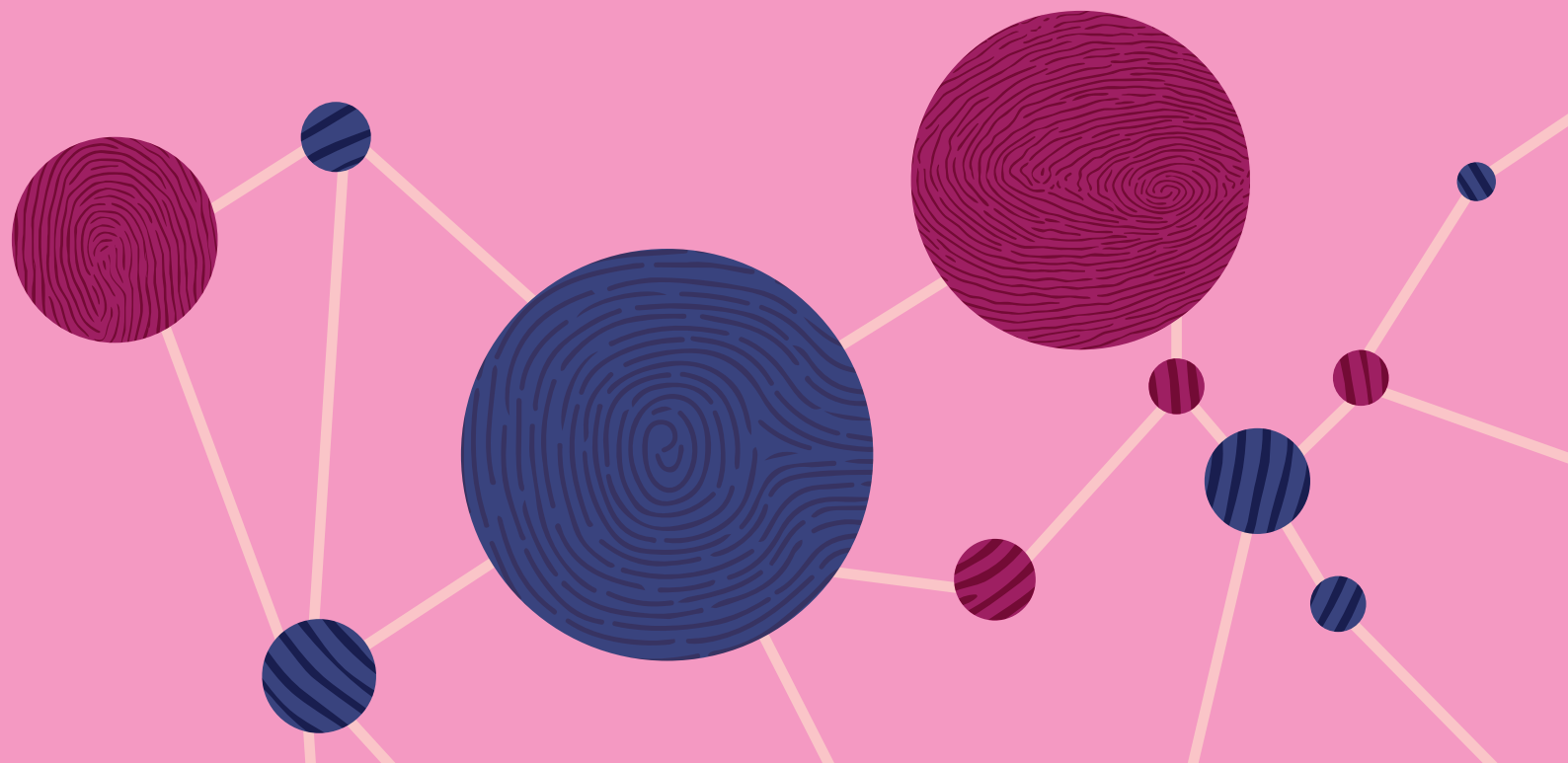
Therefore, the fundamental right to data protection, unlike the traditional meaning of privacy, is not related to a duty on the part of the state or other agents to refrain from knowing the subject. On the contrary, personal data can flow and, when it does, the flow of information must observe **contextual parameters and the informational separation of powers** in accordance with the purpose of the processing.

This is because developing a DPI and identity solutions creates a risk of violating rights, especially the protection of personal data, which is dealt with in this document. Furthermore, in an infrastructure context, it is possible that the risks generated in a DPI will manifest themselves in **other applications**, given the intense flow of data. Therefore, the introduction of **robust arrangements** is essential to ensure that this sharing of information takes place in a secure, informed and traceable manner.



04.

PROCEDURALIZING A DPI FOR THE COMMON GOOD: DATA PROTECTION AND ACCOUNTABILITY



4 Proceduralizing a DPI for the common good: data protection and accountability

Digitalization processes have given new meaning to various relationships, including those between citizens and the state, between consumers and companies, and between people and each other. Technology, incorporated into everyday processes, including public governance, brings new challenges for society in view of the asymmetry of forces between these groups[74]. Technology, especially when related to infrastructure changes, as in DPI, is associated with an interest that is not only that of the parties involved, but also involves a common good. In this digital scenario, as shown in the previous chapter, new challenges arise for the information society, since, on the one hand, data is an essential input for the development of the most varied economic and governmental activities[75], nd, on the other, its improper treatment can jeopardize the protection of fundamental rights.

Based on the key concepts related to DPI and digital identity, it can be seen that one of the pillars of DPI is what it means for this infrastructure to be public for the system itself and for its applications. The meaning of "public" in DPI can vary depending on the various elements responsible for giving meaning to this term according to what is practiced by the agents involved in building and maintaining a digital infrastructure.

As far as identity is concerned, its main functionality is to allow a person to be recognized, share their credentials or prove who they are, when necessary for interactions and transactions in the digital or offline world. Identity is one of the main applications in DPI because, in many contexts, it is necessary to identify who is using applications in the infrastructure in order to then offer the services they are entitled to. As part of the relationship becomes digital, the challenge of knowing with whom these relationships and obligations are being entered into arises once

74 COMITÊ GESTOR DA INTERNET NO BRASIL. TIC Governo Eletrônico 2019 Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação no Setor Público Brasileiro. São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2020. p. 28. Disponível em: https://cetic.br/media/docs/publicacoes/2/20200707094309/tic_governo_eletronico_2019_livro_eletronico.pdf. Acesso em: 2 dez. 2024.

75 COMITÊ GESTOR DA INTERNET NO BRASIL. TIC Governo Eletrônico 2019 Pesquisa Sobre o Uso das Tecnologias de Informação e Comunicação no Setor Público Brasileiro. São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2020. p. 30. Disponível em: https://cetic.br/media/docs/publicacoes/2/20200707094309/tic_governo_eletronico_2019_livro_eletronico.pdf. Acesso em: 2 dez. 2024.

again. This type of demand is very evident in the activities of identifying and authenticating a person carried out by the banking sector to ensure that the person carrying out a banking transaction is the account subject, or even when a person uses online spaces to request access to social security benefits.

Additional information

UK digital identity and attribute trust framework alpha v1[76]

In the context of digital identity, the UK government has published its framework with a series of parameters for establishing a secure and trusted digital identity in the region. In the UK scenario, this trust framework would be administered by a government body established by the government. However, the framework was created for agents beyond the Government, i.e. for organizations wishing to provide or consume digital identity and attribute products and services.

To this end, the government has published a document setting out the general procedures for adhering to the framework. The regulatory body is responsible for ensuring that third-party organizations follow the rules and will decide what to do if they don't, providing certificates to organizations that follow the framework. Being certified means that an organization can trust that the information it provides is accurate and reliable.

Increasingly, this identification is being conducted in DPI systems as structuring solutions for a digital society. As indicated in the first chapter of this report, various organizations are presenting different and specific descriptions and approaches to delimiting the concept of a DPI. Despite the diffusion of meanings, the definition in DPI makes it possible to draw up guidelines for the development of this infrastructure.

For this reason, the definitions of the G20 and the National Digital Government Strategy, published in Decree No. 12,069 of June 21, 2024, are relevant to understanding local and global movements on the subject of DPI.

---

76 GOV.UK. UK Digital Identity and Attributes Trust Framework Alpha v1 (0.1). GOV.UK. Disponível em: https://www.gov.uk/government/publications/the-uk-digital-identity-and-attributes-trust-framework/the-uk-digital-identity-and-attributes-trust-framework#introduction. Acesso em: 2 dez. 2024.

G20 DEFINITION

A set of shared, secure, interoperable digital systems. These systems must be able to be built on open norms and standards to deliver and provide equitable access to public and/or private services at scale. These systems must be governed by enforceable legal frameworks and rules to drive development, inclusion, innovation, trust and competition, and respect for human rights and fundamental freedoms.

This concept is only explicit in the G20 definition. It is important to recognize the interoperability and security nature of systems so that they can be used as a ground for other applications based on this foundation, infrastructure.

One of the pillars of the DPI is its open technology element, but this feature is not reinforced in the decree's definition.

"Equitable access at scale" is similar to the idea of "universal scale" in the Decree's definition.

The last part is identical. DPI should promote the respect for human rights and fundamental freedoms, so efforts should be made to understand how DPI applications affect people's rights.

DECREE DEFINITION

Digital public infrastructures - DPI: structuring solutions, transversal to various public policies, which adopt network technology standards built for the public interest, which allow universal scale, and enable the orchestration of uses by various players, from the public and private sectors, in an integrated manner in physical and digital channels, governed by applicable legal frameworks and enabling rules to promote development, inclusion, innovation, trust, competition, respect for human rights and individual freedoms.

An explicit concept only in the Decree, it reinforces DPI's commitment to the "public", which this booklet associates with the term "public value", as will be described in this topic.

The Decree's concept guarantees openness to other DPI-forming agents, not just the public sector. This understanding is in line with the concepts presented in this booklet.

Both definitions recognize the use of DPI for public and private services.

The last part is the same as the G20 definition.

Both definitions recognize the use of IPD for public and private services

At the same time as governments and organizations are maturing the concepts and applications of DPI, there are still questions about what benefits will be created by a digital infrastructure and how to evaluate it against the risks that can also arise from a scenario of digitization and intensified data flow between public and private actors. Thus, the meaning of "public" in the concept of DPI is still a matter of debate, both for academia and for the agents who develop and implement DPI applications. Initially, experts in the digital transformation of the public sector focused on issues related to the digitization of public services and the efficiency gains made possible by technology[77].

However, with technological advances and recognition of the importance of incorporating notions of public value into technological solutions for the public sector, interest has grown in defining and directing the meaning of the terms of a DPI, especially what makes it "public". In this regard, Mazzucato and others state that a DPI can be public by having technical attributes that are (i) interoperable, (ii) open-standard, (iii) open-source licenses, or (iv) with a "building-blocks" approach, in which blocks are used to generate independently scalable and improvable solutions.

On the other hand, a digital infrastructure can also be public because of its functional purposes in (i) fostering inter- and intra-community relations, (ii) improving financial inclusion and mobilizing the potential of economic agents, (iii) creating the capacities for individuals, companies and agents of society to participate and prosper in all dimensions of life, or (iv) guaranteeing the essential needs for human life, improving general well-being through impacts in the area of health, education and cultural enrichment. However, implementing the technical attributes and functions of public value is not enough to understand what makes a digital infrastructure public[78].

In an attempt to respond to the perceived shortcomings, Mazzucato states that, in addition to public value, DPI should be concerned with promoting the notion of the common good as a way of maximizing the public value created by its technical

77 Meijer, A. and Bekkers, V., 'A metatheory of e-government: Creating some order in a fragmented research field.' Government Information Quarterly, 32 (3), 237-245.

78 MAZZUCATO, Mariana; EAVES, David; VASCONCELLOS, Beatriz. Digital public infrastructure and public value: What is 'public' about DPI? UCL Institute for Innovation and Public Purpose, Working Paper Series (IIPP WP 2024- 05). Disponível em: https://www.ucl.ac.uk/bartlett/public-purpose/publications/2024/mar/digital-public-infrastructure-and--public-value-what-public-about-dpi. Acesso em: 25 abril 2024. p. 18

attributes or functions. This means that, in addition to defining the public values it aims to achieve, be they technical or functional, a DPI that effectively seeks to be "public" must follow governance parameters aligned with clearly articulated social goals among society's actors[79]. The development of a DPI is directly linked to the notion of a structure that facilitates the entry of new players and competition, mechanisms fostered in public-private partnerships.

Based on the reading proposed by Mazzucato, these governance parameters deal with (i) the capacity for co-creation and participation in infrastructure development, (ii) the direction of priorities and the role played by public authorities, (iii) the existence of transparency and accountability mechanisms, (iv) the availability of access and the benefits of DPI to the general public, as well as (v) tools for sharing learning[80].

The creation and maximization of public value is the result of a collective process built in collaboration between the sectors of society, i.e. it is not created by just one sector and fixed by the other[81]. It is from the definition of the common good that public value gains meaning and direction. In this way, DPI technologies and applications start to serve the specific purposes and objectives of the community in which they are inserted.

As a result, it can be said that the meaning of "public" in DPI is also fulfilled by other conditions, such as the implementation of personal data protection mechanisms in the infrastructure itself and the definition of procedures to guarantee the promotion of public value in DPI. This is because the preservation of the common good is achieved by guaranteeing the fundamental right to data protection, both in the content of the DPI application and in the procedure for defining its elements.

It is worth noting that this understanding of public value and the common good

---

79 MAZZUCATO, Mariana; EAVES, David; VASCONCELLOS, Beatriz. Digital public infrastructure and public value: What is 'public' about DPI? UCL Institute for Innovation and Public Purpose, Working Paper Series (IIPP WP 2024- 05). Disponível em: https://www.ucl.ac.uk/bartlett/public-purpose/publications/2024/mar/digital-public-infrastructure-and--public-value-what-public-about-dpi. Acesso em: 25 abril 2024. p. 22

80 MAZZUCATO, Mariana; EAVES, David; VASCONCELLOS, Beatriz. Digital public infrastructure and public value: What is 'public' about DPI? UCL Institute for Innovation and Public Purpose, Working Paper Series (IIPP WP 2024- 05). Disponível em: https://www.ucl.ac.uk/bartlett/public-purpose/publications/2024/mar/digital-public-infrastructure-and--public-value-what-public-about-dpi. Acesso em: 25 abril 2024. p. 22

81 MAZZUCATO, Mariana; RYAN-COLLINS, Josh. Putting value creation back into "public value": from market-fixing to market-shaping. Journal of Economic Policy Reform, 25(4): 345-360, 2022. DOI: 10.1080/17487870.2022.2053537.

is not to be confused with identifying or measuring economic value. In practical terms, simply generating economic value from the data flowing through DPI does not guarantee the achievement of public value, especially if the rights of individuals are neglected. As a result of data processing and the promotion of the common good, it is important that the **benefits** generated by the use of data are distributed fairly and equitably, and not concentrated in the hands of powerful companies or governments[82].

In this sense and based on the constitutional aspects recognized by Brazilian doctrine and jurisprudence, the development of an application in DPI, such as identity systems, and the infrastructure itself, presupposes a series of requirements for the creation and promotion of a common good, a public value.

If, on the one hand, the complexification of identity systems seeks to increase confidence in the end result, on the other hand, the lack of parameters can cause this system to jeopardize the realization of fundamental rights. Therefore, the implementation of infrastructure requires careful approaches to ensure that DPI promotes the common good. It is in this sense that this chapter aims to present **parameters** that ensure DPI applications are aligned with the DPI concept itself by guaranteeing the right to data protection and participation and accountability over the infrastructure.

4.1. Data protection as a guarantee of the common good

4.1.1. Introduction

One of the main effects of establishing a DPI is the intense flow of data, whether personal or not, passing through the digital infrastructure. DPI provides precisely the technological basis needed to enable the efficient and secure exchange of information between different systems, facilitating a continuous flow and intensive processing of data. This transit of information is within the scope of data protection regulations, especially as a fundamental right that guides the construction of an adequate information architecture.

82 VEALE, Michael. Reasons for Concern around Mariana Mazzucato's Proposals for Data Governance. Michael Veale. Disponível em: https://michae.lv/mariana-mazzucatos-proposals-for-data-governance-are-concerning/#fn7. Acesso em: 2 dez. 2024.

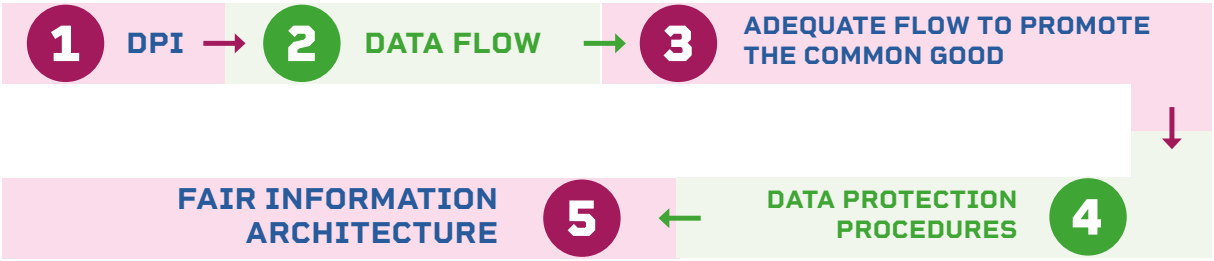
In this sense, in a DPI context, the main objects of protection are not centered solely on the parameters of confidentiality and privacy. It is based on the assumption that personal data must circulate securely and appropriately, without imposing an a priori barrier to the processing of information related to people's private lives. Furthermore, this adequate circulation of data is not limited to only data from people's intimate sphere, as was thought in a restricted concept of privacy. The consequence of data protection as an autonomous right is to ensure that only the relevant agents process a person's personal data, but it is also understood that all personal information is subject to protection, including data known to third parties or even publicly available, since the aim, in the end, is to protect the data subject, including from the violation of other rights, such as their autonomy and the free development of their personality.

Given the aim of this data protection regulatory ecosystem to preserve other people's rights, it should be noted that this regulatory framework covers all personal data that will have an impact on the data subject, not just private, intimate or sensitive information. In other words, any processing of data linked to a person that could affect their sphere of rights and interests is subject to data protection rules. People are no longer talking about protection restricted to a reductionist concept of personal data, limited to only that information with an immediate, direct and exact link to an identified person. In the ecosystem of a right to data protection, an expansionist concept of personal data is used that encompasses information with an immediate or inexact link to an identifiable person, even if indeterminate at first, but who can be identified and affected from the aggregation of information.

In this sense, it is clear that the guiding principle of the data protection framework is the measurement and analysis of the impact that the data subject will be subject to when their data is processed. In a DPI, no matter how many direct identification processes are carried out, data protection is highly stressed and must therefore be observed when processing data that affects people's access to rights and services, even if it involves anonymized or group data.

The stages of implementing a DPI are related to personal data protection tools, since data protection rules address various procedures for establishing a secure, even intense, flow of data and, with this, a fair information architecture. One of the facets of this adequate flow is precisely the promotion of a public interest, since, as the Supreme Court established in ADI 6649, there is no "dichotomous view that

places the public interest as a legal good to be protected in a totally distinct way and in confrontation with the constitutional value of privacy and protection of personal data"[83]. The public interest is promoted in the realization of the right to data protection, with its own rights and principles.



The legal obligations described in the LGPD and in the constitutional interpretation of the fundamental right to data protection proceduralize the ways of promoting the public interest and provide the necessary instruments for this to happen with legal certainty, and precisely by abandoning the idea of secrecy and consent as the only or central parameters for an adequate flow of data. It is therefore essential to comply with the procedural parameters laid down in the law so that DPI applications serve the public interest. In accordance with the third chapter of this report, the development of DPI must comply with the parameters of informational autonomy and self-determination, contextual protection and informational separation.

One of the challenges of establishing and implementing innovative solutions such as DPI is precisely the definition of accountability tools, because even if their responsibilities are not yet consolidated, the agents involved in the infrastructure must be accountable for the practices they carry out. Without the definition of **areas of responsibility**, a scenario of insecurity is created, which greatly weakens the use of DPI. People are unlikely to use and trust systems that they don't know who they are dealing with and whether they will be harmed by it.

Also, because its definition includes a multiplicity of actors collaborating in the same ecosystem, the lack of definition of responsibilities and accountability

83 SUPREMO TRIBUNAL FEDERAL. Ação Direta de Inconstitucionalidade 6.649 Distrito Federal. p. 33. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978491&ext=.pdf. Acesso em: 2 dez. 2024.

mechanisms can create a vacuum and insecurity about the rules common to all actors. An example of this is the scope of transparency rules, which are stricter for public bodies. In the context of DPIs, should these higher rules also be shared and extended to private actors who develop services in this infrastructure?

DPI users must have mechanisms in place to remedy any damage they suffer as a result of using the infrastructure. It is therefore essential that people know who they are dealing with when using DPI applications. The responsibility of each agent must be clear to the user, so that they know who to contact when they need to have their rights repaired. Defining the chain of responsibility in a DPI is complex due to the multiplicity of agents involved, but defining who is responsible for which functionality is fundamental so that the duty to repair arises only for those who caused the damage.

On the one hand, the agents involved in DPI must define when and in what way they are responsible for DPI, even if contractually, while on the other hand they cannot escape legal liability in the event of a violation of a user's right that causes damage. The definition of liability in infrastructure is especially relevant given the link between DPI and the Public Authority, which can give rise to joint and several or subsidiary liability on the part of the State[84], beyond the difference in the civil liability regime applicable to the State and private individuals.

Through a robust definition of levels of responsibility, users come to trust[85] the infrastructure and its agents, so that they understand its functionalities and encourage other people to use it too. The success of DPI also depends on the **trust** people place in it, so that if malicious agents participate in the system and obtain authentic information, people could stop using DPI to protect themselves[86].

Through a proceduralization of data protection, the aim is to arrive at an information architecture that promotes data justice and thus allows for the maximization

84 Disponível em: https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias-antigas/2017/2017-11-19_08-00_A-responsabilidade-do-Estado-e-das-concessionarias-de-servicos-publicos.aspx. Acesso em: 20 jan. 2025.

85 UNDP. The DPI Approach: A Playbook. 21 ago. 2023, p. 10. Disponível em: https://www.undp.org/publications/dpi-approach-playbook. Acesso em: 27 mar. 2024.

86 EPICENTER.WORKS. Analysis of Privacy-by-Design EU Legislation on Digital Public Infrastructures. 2024. Disponível em: https://epicenter.works/fileadmin/medienspiegel/user_upload/epicenter.works_-_DPI_Safeguards.pdf. Acesso em: 17 out. 2024. p. 5

of public value. In other words, at the end of the day, the generation of the common good depends on a contextual assessment of the information architecture that demonstrates its suitability for the data protection rules, not just described in the LGPD, but as a fundamental right.

By way of example, in order to identify and assess the public value generated by DPI, it is essential that the **information flow** of its applications, such as digital identity, is mapped and designed in accordance with data protection parameters. Only with robust, transparent data governance based on the promotion of fundamental rights is it possible to verify whether or not the public interest is being promoted[87]. This is because the value of data is highly dependent on the context and purpose for which it is used. The mere possession of data does not guarantee the generation of public value. It is crucial to consider how data is processed, analyzed and used to generate tangible social benefits.

At the same time, the flow of personal data is not considered fair only with the consent of DPI users, the architecture through which this information will transit is a component and conditioning factor of the character of justice and informational self-determination of people. Just as the data protection framework does not only apply to private and intimate data, participation and informational self-determination are not restricted to collecting the consent of the data subject.

As will be highlighted in this section, at various times in the DPI it will not even be possible to ask for the consent of the data subject for a particular processing activity, given its necessity for the execution of a public policy, compliance with a legal obligation, or the legitimate interest of the agent. Even so, mechanisms to safeguard and mitigate the risks to fundamental rights must be in place so that the data subject can preserve their self-determination and the development of their personality in general. Maintaining their capacity for self-determination is not guaranteed at a specific and isolated moment of interaction between the data subject and the DPI; this assumption must be embedded in the development of the infrastructure itself.

At the same time, as will be highlighted below, in situations where the data subject

87 VEALE, Michael. Reasons for Concern around Mariana Mazzucato's Proposals for Data Governance. Michael Veale. Disponível em: https://michae.lv/mariana-mazzucatos-proposals-for-data-governance-are-concerning/#fn7. Acesso em: 2 dez. 2024.

is asked to consent to a certain activity, in order to be able to collect free, informed and unambiguous consent, protection parameters are also needed to support this choice and offer protection to ensure that this consent is not used for another purpose, which may be incompatible, for example.

A person's self-determination will not always be realized by their consent to allow a certain agent to process certain data. In other words, the idea of the data subject's autonomy in the processing of their data is not only materialized when they consent to the processing, i.e. when it is up to the data subject to decide whether or not the processing should take place[88]. This is due to the hypervulnerability of the data subject vis-à-vis processing agents such as the Government and private companies in deciding how their data should be processed, so that they need to be empowered and given sufficient tools to emancipate them[89].

4.1.2. Legal bases

One of the elements of the personal data protection ecosystem is the definition of a legal basis for the data processing activity. Each legal basis has its own validity requirements, and it is up to the agent responsible for the processing to adopt the relevant measures to ensure compliance with the criteria that guarantee the legitimacy of the processing.

Among the hypotheses provided for in the LGPD, the options most pertinent to the DPI scenario are those of consent, execution of public policy and compliance with legal or regulatory obligations. Each of these bases has its own peculiarities that must be observed in the specific case to assess whether or not they are applicable, as will be analyzed below. In addition, each processing activity must be justified by a legal basis, i.e. for each purpose for which a group of data is processed, there must be an indication of a legal hypothesis appropriate to this purpose.

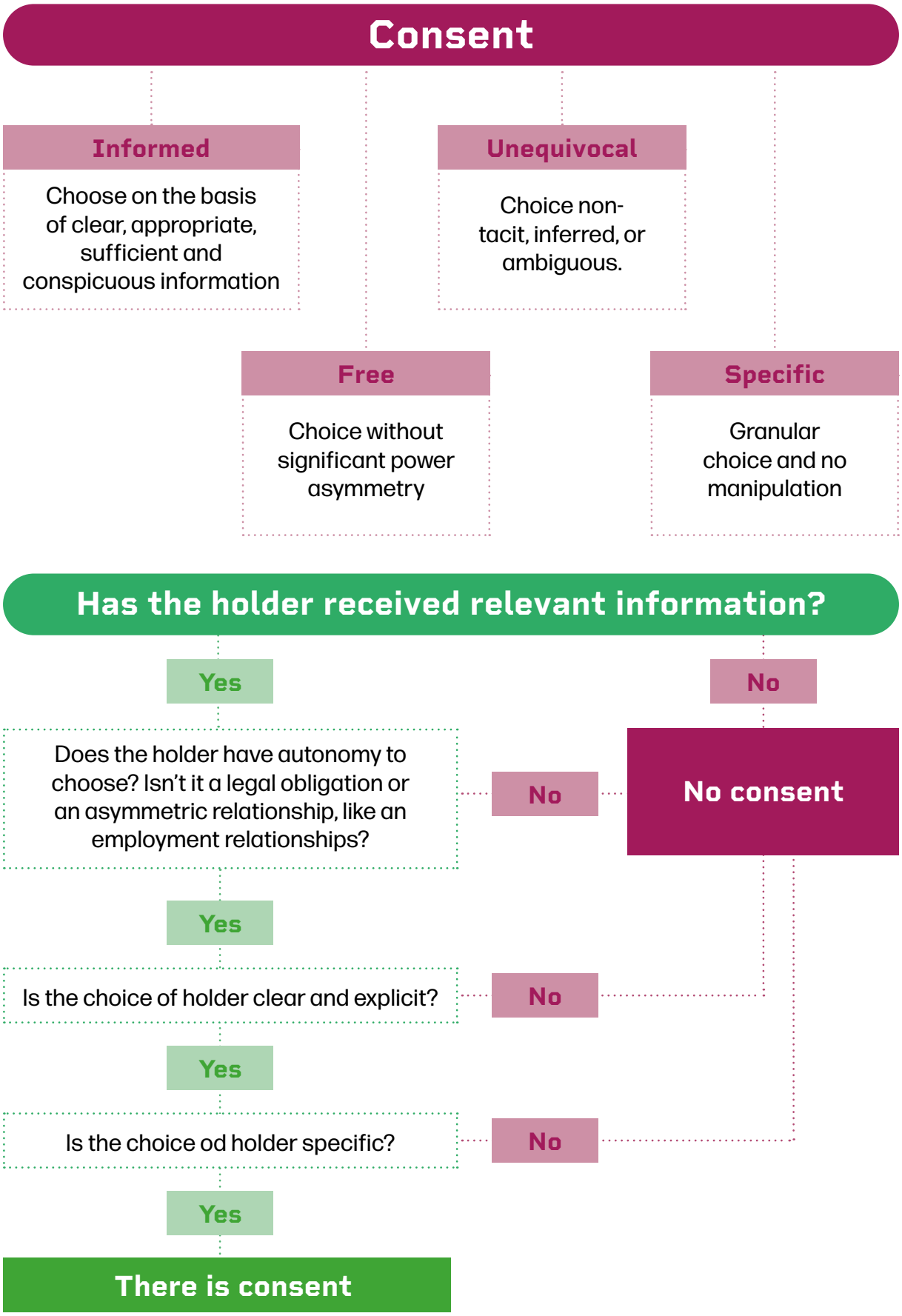
88 MENDES, Laura Schertel; FONSECA, Gabriel Campos Soares. Proteção de dados para além do consentimento: tendências de materialização. In: DONEDA, Danilo, et al. Tratado de Proteção de Dados Pessoais. Editora Forense. 2023.

89 BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 2021. Editora Forense. pág. XXVII.

Consent

Consent is the hypothesis that justifies data processing activities in which the data subject has the power to authorize or refuse. However, in order to be valid, consent must be free, informed and unambiguous, allowing the data subject to make an unconditional and conscious decision about the use of their data for a specific purpose that they are informed about. In this way, if the purpose changes during processing, the data subject must be informed and given the opportunity to provide new consent or not. Whenever consent is the legal basis chosen for processing data, the data subject must have the opportunity to revoke consent at any time, so that the agent no longer carries out that data processing activity.

Collecting the data subject's consent is a complex process in which the agent responsible for the processing has the burden of proving that it is valid and has been obtained in accordance with the LGPD. Despite the requirements for consent, it can be applied in some DPI-related cases.


Consent
Informed
Choose on the basis of clear, appropriate, sufficient and conspicuous information
Unequivocal
Choice non-tacit, inferred, or ambiguous.
Free
Choice without significant power asymmetry
Specific
Granular choice and no manipulation
Has the holder received relevant information?
Yes
No
Does the holder have autonomy to choose? Isn't it a legal obligation or an asymmetric relationship, like an employment relationships?
No
No consent
Yes
Is the choice of holder clear and explicit?
No
Yes
Is the choice od holder specific?
No
Yes
There is consent

Hypothetical example

Consent in DPI

The Federal Revenue Service in the country of the future has launched a new system that aims to make the income tax return process easier by offering taxpayers a pre-filled version based on data already available in different government databases.
On accessing the Receita Federal portal for the first time that year, taxpayer Paula came across the following message:

"Dear taxpayer,
The IRS is offering a new simplified declaration service. To use this service, we need your consent to access and use information from other government databases, including:

- Salary information (Ministry of Labor)
- Bank details (Central Bank)
- Property information (Land Registry Offices)
- Health insurance data (National Supplementary Health Agency)

This information will be used exclusively to pre-fill your tax return, facilitating the process and reducing errors. Do you agree to the use of this information for this purpose?

- ☐ Yes, I agree to share this information for the pre-filling of my tax return.
- ☐ No, I prefer to fill in my declaration manually.

You can change this preference at any time in your account settings. If you agree, the information will be stored until you submit your tax return."

Paula, after carefully reading the message and considering the benefits and implications, decided to agree to the use of her information to pre-fill the declaration.

This case illustrates how consent can be requested in a clear and specific way, giving the data subject the option of choosing whether or not to share their information for a specific purpose, in this case simplifying the tax return process."

At the same time, there are several other scenarios within the information flow of a DPI in which consent is not the most appropriate legal basis to justify data

processing, since DPI applications often cannot depend on the authorization of the data subject. This is common in cases where data is processed to operationalize public and welfare policies, generate data to evaluate the effectiveness of policies, promote public transparency, or monitor compliance with regulations. In these cases, consent cannot be free, since the processing is necessary to meet an obligation laid down by law or to serve the interests of the state. Therefore, as the collection of consent is not pertinent, other bases must underpin the processing and, together with them, other safeguards must be put in place.

Hypothetical example

Use of data without consent

Maria received a message on her cell phone. The notification informed her that she might be entitled to the new Family Support Program (PAF). The text explained that the PAF offered monthly financial aid and access to professional training courses for families in vulnerable situations. The message also explained that Maria would be able to receive the benefit because her personal registration data had been shared by the government agency she previously worked for just to check whether she could also benefit from this program, stating that after the check the data was no longer available to the PAF management body. The message suggested that Maria access the official portal or visit the nearest Social Assistance Reference Center to obtain more information and confirm her eligibility.

On the one hand, Maria was surprised by the message, since she hadn't signed up for any government programs recently. However, she soon remembered the information she had provided to the government over the years regarding registrations for social programs, her data in the last census and her informal work records. The message provided information on how the PAF's managing body found Maria, which put her mind at ease about what had happened.

This information makes it clear that the waiver of consent does not mean the waiver of adequate information. In addition, the prospect of receiving assistance and having access to training courses brought Maria relief. Maria decided to visit the welfare center the following week to get more details.

Furthermore, even if consent is not the justification for the processing, data subjects must receive a series of information about the processing. Beyond consent, data protection seeks, through the autonomy and self-determination of the data subject, a redistribution of power between data subjects and the agents who develop the infrastructure. This objective is not solely associated with an individual's ability to consent or not to processing; it is important to recognize the collective nature of data protection in DPI, given its scalar impact on different groups.

Implementation of public policies

The legal basis for the execution of public policy, on the other hand, authorizes any processing of personal data by the public administration when necessary for the execution of public policies provided for in laws, regulations or supported by contracts, agreements or similar instruments. In this case, as provided for in article 23 of the LGPD, processing must be in the public interest and serve the public purpose of the public body. Even if it is not necessary to collect the person's consent, public bodies must clearly inform which data will be shared and with whom, in addition to respecting data protection principles and rights.

Hypothetical example

Health data in DPI

The Ministry of Health has implemented a national electronic medical record system called "SaúdeConecta". This system integrated citizens' health data from various sources, including public hospitals, private clinics and pharmacies. The aim of SaúdeConecta was to improve the efficiency of the health system and the quality of patient care.

The system used the following citizen data: full name and date of birth, national identification number, medical history, including diagnoses and treatments, medical prescriptions and drug purchase records, and laboratory and imaging test results.

Based on this data, SaúdeConecta created alerts for doctors about possible dangerous drug interactions for each citizen, the system also optimized the

distribution of medicines in public pharmacies based on regional consumption and generated anonymous reports for public health policy planning

The processing of this personal data was carried out without the need for consent from the data subjects, based on the legal basis of executing public policies provided for in the data protection law. However, the Ministry of Health has implemented strict security and privacy measures, including making information available in video format, personal data access controls, data encryption, access control and regular audits. In sharing, the Ministry of Health sends data to other agents only that which is strictly necessary, anonymized or psuedonymized when possible, and delimits in a contract that these third parties cannot use the data sent by the Ministry for any other purpose, being subject to penalties and regular audits.

It's worth noting that only members of the public administration can make use of this legal basis, the law imposes a limitation on who can make use of this hypothesis. Both art. 7, IV, and art. 11, II, "b", of the LGPD, indicate the possibility of the public administration processing data for the execution of public policies. In this way, even though the DPI is made up of different actors, including private agents, the processing of personal data can only be justified on the basis of the execution of public policies if carried out by the public administration.

Compliance with legal or regulatory obligations

Furthermore, the processing of personal data will be possible whenever it is necessary to comply with a specific law or regulation. This hypothesis applies to both public authorities and the private sector. It authorizes the responsible agent to process personal information without the need for the data subject's consent, as long as the processing is strictly necessary to comply with an obligation established by law or by a regulatory body. This agent must be able to demonstrate which legal or regulatory obligation is being met through the processing of data, and the processing must be limited to what is necessary to meet that obligation. This legal basis is particularly relevant for public and private entities that need to comply with specific legal obligations, such as tax data retention, active and passive public transparency, compliance with labor standards or compliance with sectoral regulations.

Hypothetical example

Data processing to comply with the duty of transparency

The Ministry of Transparency has implemented a system called "Open Agenda" to comply with the legal obligations laid down in the rules on access to information. The system automatically collects and publishes online the agendas of all the public authorities in the agency.

Maria Silva, Executive Secretary of the Ministry, had her agenda for January 16, 2025 published in the system, including:

- 9:00 - Meeting with representatives of the company XYZ Tecnologia
- 14:00 - Hearing with the Public Servants' Union
- 16:30 - Dispatch with the Minister

The "Open Agenda" system handles the following personal data about Maria and the participants in the meetings: (i) full name; (ii) position/function; (iii) body/entity; (iv) date, time and place of the appointments; (v) general subject of the meetings.

This processing of personal data is carried out without the need for consent, based on the legal obligation of active transparency. The aim is to enable social control and prevent conflicts of interest in the exercise of public office. The system keeps the records publicly accessible for two years and then transfers them to a database in open format, as determined by the ethics committee.

In addition, the "Open Agenda" system does not provide personal information that is not in the public interest or legally binding, in order to disclose only the information necessary to ensure transparency about Maria Silva's activities as Executive Secretary of the Ministry.

Once a legal basis has been defined for each processing activity it carries out, i.e. for each purpose it aims to achieve by processing personal data, the agent responsible must comply with the requirements of this hypothesis, as well as the adequacy of the basis with the specific case and the other data protection obligations.

4.1.3. Principles

For the use of personal data in a DPI to be appropriate, there must be a mobilization of data protection **principles** to preserve informational self-determination, contextual data protection and informational separation. This means that all data processing must (i) be subject to only the minimum, necessary and adequate data, (ii) fulfill a legitimate, specific and informed purpose, (iii) be carried out only by the relevant agents, (iv) in addition to guaranteeing the rights of the data subjects, among other parameters that will be explored below.

Purpose and suitability

The principles of purpose and adequacy determine that the processing of personal data must be carried out for purposes that are legitimate, specific, explicit and informed to the data subject and, if during the processing process there is a change of purpose, the change must be compatible with the reason for which the data was used in the first instance. Thus, processing must be compatible with the purposes informed to the data subject.

These principles of purpose and adequacy are intrinsically linked to the concept of informational self-determination, which is fundamental to the protection of personal data. The ability to self-determine is associated with people's power of agency over themselves and the development of their personality and the equivalent duty of the controller to ensure that data is not used in inappropriate contexts and for purposes that are not compatible with the initial processing. However, digital identity applications can strongly stress this foundation of data protection by placing the person as an object to be identified, in which personal data from different sources and contexts, informed by the subject or not, are aggregated to form a profile that is not necessarily representative of their self-declared identity, but is what will be taken into account to validate the identity or some aspect of a person's identity.

This use of data that is not in the control of the data subject to form an identity also relates to the theory of **contextual integrity** (explored in the previous chapter). This theory advocates the protection of personal information in accordance with expectations established on the basis of contextual norms. These norms concern the context of the data subject, the sender, and the recipient of the data, as well as

the type of information that passes between these three actors, the interests of the parties, and the possibility of transmitting the data to a third party, outside the contextual field of the first collection of the data.

As a result, personal information can flow as long as it respects the expectations and circumstances of the processing, highlighting the importance of transparency and data reporting tools. These elements guarantee that the data subject will not be surprised by processing that is outside their field of knowledge and will know the necessary tools to question and hold DPI actors accountable.

The theory of informational integrity recognizes the fluid nature of privacy and data protection, which is shaped by contextual elements defined in concrete cases, so as not to indicate a simple restriction on the flow of personal information, but to understand the contextual elements of processing for appropriate data transit. By considering the context and reasonable expectations of privacy, the theory of contextual privacy[90] provides a flexible and adaptable framework for protecting privacy in an ever-evolving digital world, allowing for a dynamic and contextualized re-reading of the flow of data, including those circulating through a DPI.

90 Nota-se que no contexto norte-americano, não há diferença expressa entre privacidade e proteção de dados, como apresentado no início deste capítulo. Nesse sentido, a ideia de privacidade contextual, como apresentado pela professora Nissenbaum, deve ser entendida como em linha com a perspectiva de proteção de dados brasileira, não apenas da privacidade em si.

Tensions of the purpose principle:

CASE
Mandatory fingerprinting for electoral purposes

CONTEXT
One state's electoral court implemented a new system for taking voters' fingerprints, claiming that it would be used exclusively for identification purposes at the time of voting.

Six months after the collection, a local newspaper revealed that a private company hired to manage the biometric database was using the information to develop a commercial biometric recognition system for companies responsible for managing commercial condominiums in order to guarantee that a person identified by the condominium is the same as the one registered in the court's biometric system.

EXPLANATION
This scenario violates the principle of purpose.

The electoral court collected voters' fingerprints for the specific and declared purpose, but the company contracted to do so was conducting data processing for another purpose.

This new purpose represents a significant deviation from the original purpose. This new use not only goes beyond the initial scope of the collection, but was also not informed to the data subjects at the time of collection. Such a practice could also undermine citizens' trust in the electoral system.

CASE
Cross-checking bank data for tax inspection

CONTEXT
The Internal Revenue Service of a certain country implemented its own system and began requiring financial institutions to report all of their clients' financial transactions on a monthly basis. This included information on withdrawals, deposits and transfers, especially those that exceeded a certain amount. The aim of the system was to identify signs of tax evasion and ensure that all taxes were correctly collected.

EXPLANATION
In this case, there is no violation of the purpose principle. Even if the data collected by the financial institutions is for the purpose of carrying out the transaction, the purpose of the cross-checking of data is explicit and legitimate, as well as being informed to the data subject.

The Internal Revenue Service has established a system for collecting financial data with a clear and legitimate objective: to identify possible cases of tax evasion and ensure the correct collection of taxes. Although the data is initially collected by financial institutions for transaction purposes, subsequent use by the IRS for tax purposes is explicitly informed to the data subjects. This transparency, combined with the legitimacy of the purpose and the legal basis for such collection and use, is in line with the principle of purpose in the protection of personal data.

CASE
Use of health data for epidemiological research

CONTEXT
A university began a study on the prevalence of respiratory diseases in a certain region, collecting health data from patients seeking care at local health facilities. The researchers requested information such as medical history, previous diagnoses and demographic data from the patients, ensuring that the data would be used exclusively for epidemiological research purposes.

During the course of the study, the university researchers decided to use this data to develop a commercial application aimed at monitoring the population's respiratory health and offering telemedicine services. This use of the data was not previously informed to the participants and was not in line with the original purpose of the collection.

EXPLANATION
This scenario represents a violation of the principle of purpose.

The university initially collected health data for the specific purpose and the participants consented to the use of their data exclusively for this purpose. The researchers' subsequent decision to use this same data to develop a commercial telemedicine application constitutes a significant deviation from the original purpose. Not only was this new use not informed to the participants, but it is also not in line with the initial purpose of the collection. Such a practice compromises the ethics of the research and violates the trust of the participants.

CASE

Use of personal data for emergency notifications

CONTEXT

The Civil Defense of a state has implemented an early warning system to notify the population of emergency situations, such as floods, landslides and other natural disasters. To do this, the Civil Defense used personal data previously collected during registration for social programs and public services, such as the single registry for social programs, the registry of citizens receiving retirement benefits, and the registry of state civil servants.

Civil Defense implemented strict security measures to protect citizens' personal information, ensuring that data was only used for its intended purpose and not shared with third parties without authorization. In addition, the system enabled fast and effective communication with the population, helping to save lives and minimize damage during critical situations.

EXPLANATION

In this case, there is no violation of the principle of purpose.

Although the personal data was originally collected for other purposes, its use by Civil Defense for emergency notifications can be considered compatible with the original purpose of providing public services. The use of this data to protect lives in emergency situations serves a significant public interest, which may justify this extension of the original purpose. In addition, the implementation of strict security measures and the limitation of the use of the data to the intended purpose only demonstrate a commitment to protecting citizens' privacy. This case illustrates how, in certain circumstances, the purpose principle can be interpreted flexibly, as long as adequate safeguards are maintained.

Still intertwined with the idea of contextual data protection, the concept of **informational separation of powers** (explored in the previous chapter) reinforces the idea that data should only be accessed when there is a specific and legitimate interest in doing so. The assumption is that the state is not an informational unit and, therefore, data must flow in compliance with the competence of the body, which determines the limits and interest of the body. Thus, while the theory of contextual privacy points to the context as the benchmark for the proper treatment and flow of data, the theory of informational separation has the definition of the functions and authorities that access the data as the benchmark for defining the legitimacy of the flow of data.

In the context of DPI, an infrastructure that recognizes an informational separation implies a differentiation between which information can be accessed by which entities, in view of their functions and competencies. As one of the basic applications of DPI, the use of identity data, beyond simple identity verification and authentication, has the potential to become an almost continuous measurement of people's daily lives through the collection, processing and sharing of their personal data[91], as a way of monitoring the evolution of their own personality

Hypothetical example

Reusing data in different contexts

Sofia Oliveira was a single mother of two living in a low-income neighborhood. Sofia worked as a day laborer, with an unstable income that was insufficient to support her family.

In March 2003, Sofia visited her town's Social Assistance Center and, in order to access the municipality's benefits, she filled out an extensive digital form, providing detailed information such as her employment history over the last five years, average monthly income, data on the absence of the children's father, current and previous addresses and information on her family support network.

91 BODY AND DATA. Digitization of Identity in Nepal: Efforts, Experiences and Effects. 2023. Disponível em: https://bodyanddata.org/wp-content/uploads/2023/10/BiometricReport_2023_07_31_Final_compressed.pdf. Acesso em: 12 jan. 2025.

Sofia was told that this data would be used exclusively to assess her eligibility for assistance programs. As a result, she began to receive housing assistance and food vouchers, which have been crucial to improving her family's quality of life.

In 2025, the city's Department of Public Safety implemented a new predictive crime prevention system. This system, developed by a technology company with no experience in social policy, uses machine learning algorithms to identify "high-risk zones" and "individuals prone to criminal activity".

In order to reduce crime in the city, the president of the Social Welfare Center agreed to share the beneficiaries' data with the security department. Thus, without the citizens' knowledge or consent, the Social Security database was integrated into the system. The algorithm assigned risk scores based on factors such as financial instability, residence in high-crime areas, the absence of a father figure in the home, and the frequency of changes of address.

Shortly after sharing this information, Sofia was surprised by a police raid on her home. The officers, armed with a warrant based on the analysis of the prediction system, searched her home, questioning her about her "criminal connections". The children, frightened, cried as the officers searched their belongings.

In the following months, Sofia faced frequent police visits, usually in the early hours of the morning or late at night, as well as overt surveillance at her place of work, leading to the loss of clients, bullying from children at school, labeled as "children of criminals", and difficulties in renting a new apartment due to the "criminal record" generated by the system.

Sofia's case was only re-evaluated by an independent audit of the system that revealed its serious biases and privacy violations. Although she was officially cleared, the damage to her reputation and well-being had already taken place.

It is essential to recognize and guarantee specific levels of information to the agents that make up a DPI. In other words, the infrastructure itself should not form an informational unit, putting all agents on an equal footing when it comes to accessing and processing the personal data available on the DPI. As much as there are arguments in defence of supposed efficiency, plans to link the data available on the DPI with other public and private organizations should be evaluated with caution because they could impact people in various spheres of their lives.

An efficient system is not one that has indiscriminate access to data available for any purpose, but rather a system that has robust governance of this data, following the precepts of data protection to process only appropriate and necessary data. Likewise, there is no dichotomy between the realization of the public interest and the guarantee of data protection. As a result, the public interest should not be understood "as a legal good to be protected in a totally different way and in confrontation with the constitutional value of privacy and protection of personal data"[92]. Thus, the execution of the public interest is in line with proper data protection, especially in the definition of specific purposes known to the data subject.

Data minimization

The principle of necessity, or data minimization, requires that the personal data processed be limited to the minimum necessary to fulfill the purposes that justify their use. This principle restricts processing to data that is relevant, proportionate and not excessive in relation to the purposes, so as to allow the agents responsible to only collect and process data that is essential and indispensable for the purpose sought.

This principle can be exemplified by notions already consolidated in the context of identity through the concepts of **"zero-knowledge" and selective openness of data**[93]. These concepts function as a way of verifying whether certain attributes or combinations of attributes of a person are true. A simple example is verifying

92 SUPREMO TRIBUNAL FEDERAL. Ação Direta de Inconstitucionalidade 6.649 Distrito Federal. p. 56. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978491&ext=.pdf. Acesso em: 2 dez. 2024.

93 EPICENTER.WORKS. Analysis of Privacy-by-Design EU Legislation on Digital Public Infrastructures. 2024. Disponível em: https://epicenter.works/fileadmin/medienspiegel/user_upload/epicenter.works_-_DPI_Safeguards.pdf. Acesso em: 17 out. 2024. p. 8

that a person is of legal age without revealing their date of birth. This has become a standard for modern digital identity systems and is a precondition for making DPI systems compliant with modern data protection standards. Zero-knowledge can also prevent the user from being linked in interactions with the same or a different trusted party in all cases where full user identification is not required.

Hypothetical example

Access to age-verified spaces

Mariana goes to the same nightclub every Friday and the agent who checks her age doesn't know that she's the same person as in previous weeks. This is because she only shares with the agent the validation of her age and not her name, profile picture or social security number. Finally, whenever a trusted party, i.e. the nightclub representative, requests information from Mariana, she needs to be able to share all the data, none of it or "selectively disclose" only parts of the information that has been requested.

It is in this sense that the development of customizable data control features is seen as another management tool and privacy settings, allowing users to easily adjust their data sharing preferences. At the same time, integrating different databases by sharing them widely is not the only solution for exchanging information and validations. Logical integration allows only the data needed for a specific purpose to be accessed or exchanged, reducing the risk of unnecessary exposure of information and enabling more precise control over what data is shared.

In addition, functionalities such as data export and deletion requests can give people control over their personal information. These individual control tools are just one part of the equation for guaranteeing the right to data protection. It is up to the processing agent to add other elements to this equation in order to manage risks in a shared way, since agents also control the data and therefore the risks associated with processing.

First Thoughts

What data is disproportionate for a particular processing of personal data?

One of the main tensions in the use of data for identification in a DPI is the definition of what personal data is necessary to identify someone. On the one hand, some argue that the greater quantity and variety of data guarantees greater confidence in the identification process, while others point out that too much data, especially out of context, can jeopardize the final result. Therefore, defining what data is needed to identify someone is fundamental to guaranteeing the effectiveness of the process itself.

A similar issue has already been faced during the discussion on what personal data can and cannot be used to define a credit score. The Cadastro Positivo Law, No. 12.414, prohibits information from being taken into account when composing a credit score:

- that are not linked to credit risk analysis and those related to social and ethnic origin, health, genetic information, gender and political, religious and philosophical beliefs;
- of people who do not have a first-degree relationship of kinship or economic dependence with the registrant;
- related to the regular exercise of rights by the registered person, as provided for in item II of the caput of art. 5 of this Law.

In other words, in this case, the law has defined information that is considered excessive and therefore cannot be used to define a credit score. The same question arises in the context of identity: what data is needed to assess whether a person is a possible fraudster when identified to access a social assistance program, for example? If, in the logic of big data, all data can potentially be useful for identifying someone, it is necessary to define parameters of need that are not only guided by technical elements, but also by elements of justice.

It is in this sense that this Report points to the need to observe minimum pa-

rameters for a fair flow of data, such as the implementation of informational separation practices and contextual protection for the promotion of public value and an autonomous development of the personality of DPI users.

Informational separation implies keeping data sets collected for different purposes distinct, avoiding indiscriminate cross-referencing of information that can lead to invasive or unfair inferences. Contextual protection aims to ensure that data is only used in the context for which it was originally collected, respecting individuals' reasonable expectations of privacy. These practices are fundamental to balancing the need for effective identification with the protection of individual and collective rights. They help prevent the excessive or inappropriate use of personal data, which could result in discrimination, breach of privacy or other harm to data subjects.

As an example, in a contextual analysis for access to a social program, it may not be reasonable to process data on people who have no direct relationship with a beneficiary, such as relatives who are not economic dependents, or information related to the regular exercise of rights by the citizen, such as participation in unions or associations.

In addition to this critical analysis of the specific need for each piece of data processed to achieve a certain purpose, the principle of necessity is also a normative command for agents to always use the least intrusive forms and methods of processing possible to achieve that purpose[94]. In this way, it is up to the agent responsible to assess whether there are other, less costly and less risky ways for data subjects.

Transparency and open access

Just as the principles of purpose and adequacy are closely associated with the concepts of personality development, contextual protection and informational separation, the principles of transparency and free access are also impacted by these notions. The principle of transparency guarantees data subjects access to

94 ANPD. Hipóteses legais de tratamento de dados pessoais Legítimo Interesse. 2024. Disponível em: https://www.gov.br/anpd/pt-br/centrais-de-conteudo/materiais-educativos-e-publicacoes/guia_legitimo_interesse.pdf. Acesso em: 5 fev. 2025.

clear, precise and easily accessible information about the processing and the respective processing agents. The principle of free access guarantees data subjects the possibility of an easy and free consultation on the form and duration of the processing, as well as on the completeness of their personal data.

In order to be able to measure the contextual expectations of data subjects and thus assess whether their rights have been violated, it is essential to analyze the level of transparency granted to them by the agent responsible for processing. This is because if the DPI user receives the relevant information about the processing and is aware of the data flow, they are unlikely to be surprised by how the DPI works. Privacy as contextual integrity is also guaranteed by the principle of transparency, since the expectations of data subjects are aligned and formed on the basis of the information they receive.

In the same vein, the STF decisions analyzed in this report reinforce the government's commitment to provide transparency about the sharing it carries out, and it is up to the agency to provide transparency about the personal data processing activities it carries out.

Parameters for public authorities to share data according to the STF

The sharing body must comply with the LGPD:

Full compliance with the requirements, guarantees and procedures set out in the LGPD, insofar as this is compatible with the public sector. Use of electronic security and access registration systems, including for accountability purposes in the event of abuse.

The body must publicize the processing it carries out: the obligation of the public body to give due publicity to the cases in which each government entity shares or has access to personal databases.

The sharing body must publicize the sharing:

A formal administrative procedure must be set up, accompanied by prior and exhaustive motivation, to allow the Judiciary to control its legality.

The sharing body must assess the risks of sharing:

Assessment of the compatibility of data sharing, verifying whether sharing personal data to another public body for a purpose other than that initially declared undermines the authorization of the data subjects. Adoption of measures that are proportionate and strictly necessary to serve the public interest.

Based on this information, data subjects, who are DPI users, now have adequate tools to understand, decide and question with greater autonomy about the processing of their personal data and its impacts, including on the development of their personality.

Hypothetical example

Transparency as a tool for DPI users

In 2030, the federal government implemented a DPI called the "Citizen Data Transparency Portal" (PTDC). This portal allows any citizen to access information about how their personal data is being used by different government agencies.

Through individualized access, each user accesses the portal using their digital identity and can see which bodies have access to which types of their personal data. The portal also allows the user to see a record of when and by whom the data was accessed, as well as the stated purpose for using the data. The portal offers a system for citizens to question the use of their data directly to the bodies responsible.

Accessing this portal, Mônica, a DPI user, accesses the PTDC and discovers that her health data has been accessed by the IRS. Intrigued, she uses the portal's questioning mechanism to ask why the IRS has accessed her health data.

The IRS replies within an established timeframe, explaining that the access was made to check whether Mônica can claim an income tax refund because of the health insurance payment. Mônica, not satisfied with the explanation, believing that the proof of health insurance enrollment would be sufficient for this purpose, can then request more information, ask for the data to be recti-

fied or deleted if she considers that it is being used improperly, or file a formal complaint if she believes that her rights have been violated.

As a result of this questioning, the IRS will re-evaluate whether it is necessary for it to access citizens' health data. This advance was only possible because, in addition to providing information, the principle of transparency also empowers citizens to be active agents in protecting their personal data.

Also, from the point of view of the LGPD, specifically for the Public Authorities, the law reinforces the duty of publicity in relation to the processing of personal data carried out by the public administration, also in line with the principles of impersonality and publicity of the public administration provided for in art. 37 of the Federal Constitution. According to art. 23, I, of the LGPD, it is up to legal entities governed by public law to provide "clear and up-to-date information on the legal provision, purpose, procedures and practices used to carry out these activities, in easily accessible vehicles, preferably on their websites". In cases of data sharing, it is good practice for public agents to formalize this processing by signing a contract, agreement or similar instrument[95].

Non-discrimination

The principle of non-discrimination makes it impossible to process personal data for unlawful or abusive discriminatory purposes. In the context of DPI, especially digital identity, this principle is crucial to ensure that the processing of personal data is carried out in an ethical and respectful manner, protecting individuals against unlawful or abusive practices of discrimination that may arise from the misuse of their personal information, even if indirectly or unintentionally. The aim of this principle is to ensure that personal information is not used to perpetuate existing prejudices and inequalities.

95 ANPD. Guia Orientativo de Tratamento de dados pessoais pelo Poder Público. 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 20 dez. 2024.

Hypothetical example

Automated system with discriminatory effects

A housing credit assessment system has been implemented in the City of Data. Its aim is to assess citizens' eligibility for social housing programs based on their identity data. To do this, the system uses citizens' digital identity data, including employment history, income, address and credit history. Based on this information, the system determines the likelihood of an applicant meeting their housing loan payments, information that is used to automatically approve or reject loan applications.

After a year of operation, an independent audit revealed that candidates from certain historically marginalized urban areas had a significantly higher rejection rate, even when other factors were similar. Also, women, especially single mothers, were approved less often than men with similar financial profiles.

It was soon realized that the system was trained with historical data that reflected pre-existing discriminatory patterns in the real estate market. The system used apparently neutral variables, such as postal code, to infer protected characteristics, such as race. An academic article by Ramon Vilarino and Renato Vicente demonstrates how the use of location information introduces racial bias into a credit scoring model, even though this information is not directly given to the model[96].

These issues were not noticed during the development of the system because the team responsible for the system was not diverse enough to identify potential biases and these requirements were not considered. Because of these flaws, the system reinforced existing patterns of housing segregation and economic inequality. The revelation of these problems led to a significant loss of confidence in the social housing program and in the use of technology for government decision-making.

96 VILARINO, Ramon; VICENTE, Renato. An experiment on the mechanisms of racial bias in ML-based credit scoring in Brazil. arXiv preprint arXiv:2011.09865, 2020.

Digital public infrastructure applications must therefore be proactively tested before they are implemented to ensure that they do not generate discrimination, and can even rely on external audits and public reports, as will be discussed in the next section. These tests allow risks to be identified and mitigated before they become real problems, saving resources and protecting infrastructure users.

4.1.4. Subject's rights

The rights of data subjects represent the most robust and direct aspect of the LGPD for the exercise of informational self-determination. This set of rights provides data subjects with tools so that they can know and interfere in the processing of their personal information, including allowing them to make informed decisions about the use of their data. Informational self-determination is therefore not just an abstract concept, but a practical right that can be exercised through the mechanisms established by the LGPD.

While the principles and legal bases of the LGPD create a general framework of obligations for data controllers, the rights of data subjects are the practical instruments through which people can not only demand compliance with these obligations, but also actively exercise their informational self-determination. These rights enable data subjects to question, modify and even revoke the use of their personal data, placing them at the center of the information processing process.

In the field of data protection, even in the context of DPI, the data subject has the right to know a range of information, such as what personal data is in DPI applications, who accesses it and what their responsibilities are, for how long, for what purpose, and with whom they share it, according to article 9 of the LGPD. In addition, DPI users must receive information about their rights as data subjects and the manner in which their data is processed.

Specifically, data subjects can: (i) request confirmation that their personal data is being processed by a given DPI application, (ii) access the personal data that is processed, (iii) request the correction of incomplete, incorrect or outdated data, (iv) request the anonymization, blocking and deletion of data that is unnecessary, excessive and/or processed in non-compliance with the LGPD, (v) request information on the public and private entities with which the company shares data, (vi) request the portability of their data to another service or product provider, observing commercial

and industrial secrets, and (vii) oppose the processing carried out on the basis of one of the hypotheses of waiver of consent, in case of non-compliance with the LGPD.

Furthermore, when the legal basis justifying processing is consent, the data subject may (viii) not provide consent, (ix) revoke consent at any time by means of a free and simplified procedure, and (x) request the deletion of data processed on the basis of consent, except when necessary for compliance with a legal or regulatory obligation by the controller; study by a research body, guaranteeing the anonymization of the data; transfer to a third party; or exclusive use by the controller, with access by a third party prohibited, and provided that the data is anonymized.

When automated decisions are used, the data subject has the right to (xi) request a review of decisions that affect their interests and (xii) obtain clear and adequate information about the criteria and procedures used for automated decisions.

First Thoughts

Automated decisions in the formation of an identity

Identity processes are increasingly embracing profiling practices and automated decisions to define the probability of a person being who they say they are or possessing an attribute or characteristic, either through a layered identity or through the massive use of data.

As argued earlier, DPI applications can put a strain on people's capacity for informational self-determination, free personality development and autonomy. Processes such as profiling aim precisely to infer preferences, attitudes, behaviors or future events based solely on the correlation of captured and inferred data, without taking into account personal accounts and narrative claims, which can greatly limit the opportunities granted to people and the way they act. This is because these systems aim to predict and infer possible behaviors in the future and direct people precisely towards these possibilities, defining a pattern of appropriate and expected behaviors. This pattern-setting can lead to the systematization of discrimination and injustice, threatening the fundamental rights of people who have not actually taken any action contrary to what is expected, but who have been identified by an automated system as having a high probability of doing so.

In this same context of automated decisions for identification, probabilistic logic is also being applied, which means that systems no longer seek absolute and unequivocal identification of individuals, but work with acceptable degrees of probability and margins of error. This approach implies that decisions are made based on statistical inferences and data correlations, rather than certainties about a person's identity or characteristics. Thus, people lose visibility of how their data is being used for identification. This means that they stop playing an active role in being identified and become the object of identification, without knowing what information has been used to form their identity.

In the face of these new identification practices, the rights of the holders emerge as tools to balance these practices with people's capacity for self-determination. These rights allow identity to be created not just by a monologue from the identifying party, but a dialog between the identifying party and the identified party. Specifically, the right to obtain information about the criteria and procedures used is an instrument for understanding the automated decision-making process and, with this, guaranteeing the other rights of the data subject, such as contesting and requesting a review of the decision based on the information provided.

The two rights aim to "balance the distribution of powers in decision-making in order to ensure that the data subject participates proportionately in the decision-making process that affects their interests"[97]. Therefore, in the context of identity as DPI, the subject can use these rights for tools so that he knows the elements that make up his identity and, with this information, can oppose and request revision of these elements.

It is worth noting that two rights apply even in the case of intermediate decisions. As a rule, an automated decision-making process is divided into several stages, which may or may not include the participation of a person to make the final decision, and some might argue that this right only exists when the final decision is not human. However, the LGPD opens up "greater scope for automated treatments to be considered as decision-making pro-

97 ALMEIDA, Eduarda Costa. Diga-me os seus dados, que eu lhe direi quem você vai ser: o Direito à explicação como garantia da autodeterminação informativa na Lei Geral de Proteção de Dados Pessoais. 2023. 168 f., il. Trabalho de Conclusão de Curso (Bacharelado em Direito) – Universidade de Brasília, Brasília, 2023.

cesses, even if they are not the last point in a decision tree"[98]. Therefore, people can request these rights in a DPI, even if the automated decision is not final, but affects their interests and fundamental rights.

This information must be disclosed through clear, simple and accessible materials. This obligation is in line with the duty of transparency and information on the processing of personal data in the infrastructure. In this sense, the implementation of **accessible channels to address the rights of data subjects, support and complaints** is essential to ensure that citizens can register complaints and problems faced when using the DPI. These channels facilitate and speed up the identification of faults or vulnerabilities in the system, which increases the responsiveness of the infrastructure and, consequently, increases user confidence in the DPI.

These channels must be inclusive and accessible to anyone, whether digitally or physically, including those with restricted access to DPI. Given the complexity of the actors that make up the DPI, the agents responsible for data processing must agree among themselves who will be responsible for attending to the rights of data subjects, ensuring that all requests are duly dealt with and responded to. It is equally important to establish clear deadlines for responding to and resolving problems, ensuring that people feel that their concerns are being treated seriously.

The DPO is the agent responsible for responding to requests from data subjects, as well as receiving communications from the national authority, among other things. This officer is appointed by the agent responsible for the processing, i.e. every agent who decides on aspects of data processing must have an officer. In the public sector, this means that the obligations of the agent responsible "are exercised by the public bodies that carry out functions on behalf of the legal entity of which they are part, a phenomenon that characterizes the internal distribution of competences"[99]. Therefore, it is up to the public body that processes data to comply with the LGPD,

98 MARTINS, Pedro Bastos Lobo. A regulação do profiling na lei geral de proteção de dados: o livre desenvolvimento da personalidade em face da governamentalidade algorítmica. Dissertação (mestrado) - Universidade Federal de Minas Gerais, Faculdade de Direito, 2021, p. 77. Disponível em: https://repositorio.ufmg.br/bitstream/1843/43900/4/Pedro%20Martins%20-%20Disserta%C3%A7%C3%A3o%20-%20A%20REGULA%C3%87%C3%83O%20DO%20PROFILING%20NA%20LEI%20GERAL%20DE%20PROTE%C3%87%C3%83O%20DE%20DADOS%20o%20livre%20desenvolvimento%20da%20personalidade%20em%20face%20da%20governamentalidade%20algor%C3%ADtmica.pdf. Acesso em: 28 jun. 2024.

99 ANPD. Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado. 2021. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/2021.05.27GuiaAgentesdeTratamento_Final.pdf. Acesso em: 20 jan. 2025.

including by appointing a person in charge.

Hypothetical example

Updating data in a DPI

Marília, a user of a health DPI application, recently underwent new medical tests which showed different results to those recorded in the system. These most recent tests are not registered in the infrastructure because they were carried out at a clinic not linked to this application, but she should update her data in the application in order to be able to schedule a medical appointment to analyze the test results. In order to update her information, she decides to exercise her right to change personal data, specifically medical data.

Initially, Marília tries to update her information via the health app on her smartphone. However, she realizes that there is no option to manually update test results. In addition, the DPI application is made up of various agents, such as the Ministry of Health, which is responsible for the overall management of the system, public and private hospitals, which provide care data, laboratories, which share test results, as well as the DPI identification platform, which provides digital authentication of users.

Faced with so many agents, Marília looks for the contact person in charge of these agents so that she can claim her right. However, she only finds the contact details for the DPI identification platform. Frustrated, Marília finds no clear guidance on how to proceed. She tries to contact her doctor, but is told that he is not allowed to change the data on the DPI.

Marília then decides to contact the person in charge of the DPI application identification platform. After several transfers, she is told that she needs to contact the health institution that carried out the original tests. However, when Marília explains that the new tests were carried out in a different laboratory, the attendant doesn't know how to proceed and Marília ends up not knowing where to turn.

This scenario highlights the need for a clear and accessible point of contact

for users who need to update their data in the DPI, as well as well-defined procedures for updating information and greater transparency and education for users about their rights and the processes related to managing their health data in the DPI. Marília's situation illustrates how exercising the rights of data subjects is beneficial for all the agents that make up the DPI and for the very functioning of the infrastructure.

User experience is a crucial factor. Participating agents can provide valuable insights into the usability and accessibility of systems, ensuring that DPI meets people's real needs. Building a fair and citizen-friendly DPI depends on digital inclusion, allowing all segments of society to have access to the infrastructure. Involving the community in the development of DPI increases transparency and, consequently, **trust** in public institutions and in the digital infrastructure itself.

Systematically collecting feedback and monitoring changes in people's ability to navigate the DPI are essential to evaluating the system's effectiveness. Carrying out regular user satisfaction surveys, as well as implementing metrics to assess ease of use and navigation, allows areas for improvement to be identified. Even after the solution has been developed, participatory monitoring is essential for the DPI to function properly.

The following example illustrates how DPI identity application can stress data protection elements:

TENSIONS BETWEEN DPI IDENTITY AND DATA PROTECTION TOOLS	
Elements of identity	**Data protection tensions**
John has an identity card in his name, identifying him with his biometrics, photo, full name, CPF, sex, date of birth, filiation, place of birth and nationality, as well as the issuing body and place of issue of the identity card.	The issuance of an identity document is one of the most frequent requirements for accessing essential or non-essential services and products, such as bank accounts, social benefits, leisure facilities and others. As a rule, this document is issued by the Government and used by other agents, public or private, in various contexts. As a rule, identity data is shared in an unlimited and untraceable way, i.e. the document and all its data is sent to third parties, even its copy, without it being possible to record with which agents the information has been shared and the associated context.
When John turns 18, he has to file an income tax return. To file his income tax return, John registers on his country's government portal and authorizes the tax authorities to use his data to issue a pre-filled tax return	The separation of information indicates a scenario in which the body responsible for taxes does not have the same information as the body responsible for issuing the identity card, since the purpose of the processing is different. At the same time, knowing the difference in competence of the bodies, it is up to the subject to authorize this flow.
When John loses his job as a truck driver, he registers with the government's social program registry as a requirement to receive social assistance from the government. This registration is done through his government portal account.	Identity, as one of the tools for accessing social benefits, is used by the social welfare agency. To do so, citizens may have to access the government portal as the digital aspect of its services. The registration made by the citizen is made in a certain context, which delimits the form and guidelines of data processing to guarantee their autonomy as a subject of rights.

When John opens an account with a bank in order to get credit to start a business, he registers with the bank through the state portal, which only transmits the information that is essential for the bank to be able to identify John and validate his identity and registration details. When he applies for a loan, João is denied. Some of the reasons for the denial are the fact that João is on the register for social programs, which would indicate a situation of financial vulnerability, and the information that João declared himself exempt from income tax four years ago. This information was accessed by the bank through the portal. João was unable to challenge the decision because there was no transparency mechanism to inform him of the reasons for the loan being denied and no system for reviewing the decision. João is no longer included in the social assistance register that he previously received and does not declare income tax, as all his income comes from informal professional work, and he is looking to formalize his enterprise with this loan.	In order to validate their identity, it may not be necessary to share all the data related to a person's identity. In this case, sharing the data or validating it can be done as a way of minimizing the processing carried out by other agents, such as a banking institution. However, the sharing or simple communication of data between agents who have different purposes and competencies can indicate a violation of principles such as informational separation and contextual protection, affecting the autonomy and development of a person's personality. In this case, the bank accesses information known to the body responsible for issuing IDs and the body responsible for taxes. The data processed by each agent takes place in a certain context and relates to a specific situation, and communication between agents is not necessarily pertinent, useful or effective, as in the definition of access to credit. Despite this, if data is communicated, mechanisms for information, challenge and review of this data exchange are essential to guarantee the autonomy of the individual. This is because access to certain products and services is based on the exchange of data. These mechanisms for opposing the communication or its effects are a basic tool for minimizing the negative effects of this treatment, guaranteeing a fair flow of data.

João registers on a private job search platform, and logs in through the government portal, which initially only provides João's name and CPF, guaranteeing his identification to the platform, which requests additional registration data such as email and educational and professional history. When applying for a job as a truck driver on this platform, the application process asks for validation of identity through the portal, and requests authorization to access other data on the portal, including data relating to João's financial transactions, since the employer will pay for the insurance of the truck that João will be driving. João's application is rejected. The information regarding his registration in the register for social programs and his credit score were determining factors for this decision.	Identity information linked to the citizen can now flow for the purposes of access to work, beyond simply validating their identity. Again, the lack of opposition mechanisms can harm the citizen. The context of the processing may not be taken into account, by not observing the social sphere of the processing of the subject, as a citizen and not a future employee, the recipient of the information, as well as the type of data shared and the expectations defined by the context of identification. In this case, the violation of data protection parameters in the relationship of identity and access to social benefits takes on a new layer when a new relationship is added, that of employment. It is worth highlighting the possibility of the data subject authorizing the job search platform to access data processed by the authority responsible for the identity. Although the citizen may not authorize it, it is recognized that they are vulnerable to the impact of not authorizing it, which is the denial of a job offer. As much as there is room for non-authorization, it is possible to question how free this consent would be

John returns to a situation of financial vulnerability and applies again to be included in the social assistance program. When making this application, João is asked to send a high-quality photo of his face and ID card. This was because the fraud detection system indicated a sign of fraud in João's application. This anti-fraud system is operated by the same company that provides credit scoring services for the bank that denied John a loan. John's cell phone has a broken camera and there are no face-to-face service points in the rural district where he lives.	In a DPI context, the lack of realization of the right to personal data protection through contextual protection tools and informational separation affects the citizen's ability to develop their personality. The effect of this violation becomes more complex as it creates layers of applications that communicate with each other and thus communicate their vulnerabilities. In a context of digitalization without DPI, the system's faults and vulnerabilities could have local or little cross-cutting impact. However, the development of a digital infrastructure makes it possible for different applications to have implications for each other, which makes it possible for these faults to be transmitted. In this scenario, the need for effective protection tools is even more essential if the system is to function properly in accordance with people's rights.

In view of the tensions between data protection and the development of identity solutions, **impact assessments** are fundamental tools in structuring this information architecture. The aim of the assessment is, by mapping and anticipating the possible risks of an application, to help make informed decisions and protect social interests[100]. This is because even before negative events occur, including the violation of rights, the organizations that conduct these assessments are already actively seeking to minimize the likelihood of them occurring and adopt more protective safeguards.

In addition, impact assessments also function as accountability tools for the agents involved in developing the systems. Even before they are made available for general use, it is already possible to understand what practices will be adopted to address and minimize the risks identified. The drafting and review of this report strengthens the idea of **procedural justice[101]**, since it is not just about obtaining a fair result, but also a fair path to that result.[102].

In the context of identity systems, impact assessments can function as a strategic tool to ensure that the identity application is adequate for data protection, given the **high risk of data processing[103].** Identity systems, especially in the context of DPI, aim to be accessible to a large number of people, giving rise to large-scale processing of personal data, as well as significantly affecting the interests and rights of these people. It is through identity that people access a series of rights and benefits.

Given the risks involved in DPI identity system, the development of a system in conjunction with an impact report covering possible impacts on the fundamental rights and freedoms of individuals and groups is useful for mapping and measuring

---

100 KLOZA, Dariusz et al. Avaliações de impacto sobre a proteção de dados na União Europeia: complementando o novo regime jurídico em direção a uma proteção mais robusta dos indivíduos. d.pia.lab Policy Brief, 1/2017, 2020.

101 KLOZA, Dariusz. Privacy Impact Assessments as a Means to Achieve the Objectives of Procedural Justice. Jusletter IT. Die Zeitschrift für IT und Recht, 2014. Disponível em: https://researchportal.vub.be/en/publications/priva-cy-impact-assessments-as-a-means-to-achieve-the-objectives-o. Acesso em: 11 mai. de 2024.

102 KLOZA, Dariusz. Privacy Impact Assessments as a Means to Achieve the Objectives of Procedural Justice. Jusletter IT. Die Zeitschrift für IT und Recht, 2014. Disponível em: https://researchportal.vub.be/en/publications/priva-cy-impact-assessments-as-a-means-to-achieve-the-objectives-o. Acesso em: 11 mai. de 2024.

103 BIONI, Bruno; GARROTE, Marina; MEIRA, Marina; PASCHOALINI, Nathan. Entre a visibilidade e a exclusão: um mapeamento dos riscos da Identificação Civil Nacional e do uso de sua base de dados para a plataforma gov.br. Associação Data Privacy Brasil de Pesquisa, 2022.

these risks. This assessment can be made **public** before any data processing[104], so that there is room for analysis and discussion of the risks to be addressed. This assessment can include a survey of appropriate safeguards to limit and mitigate the risks identified.

It is worth noting that the development of an impact report makes it evident how personal data protection guidelines emerge as useful tools in the development and implementation of identity systems in a DPI, avoiding the retention of unnecessary data and ensuring **secure and non-abusive data sharing**. This reinforces the notion of data protection parameters functioning as relevant tools in the realization of the common good, an essential requirement for perceiving a digital application as part of a DPI.

4.2. Accountability and participation in DPI

4.2.1. Accountability for prevention and precaution

The regulatory rationale of the General Data Protection Law follows a logic of prevention, i.e. seeking to protect data subjects before the damage occurs and adopting measures to prevent it from happening, which is why it is called *ex ante*. The idea is that regulating and creating sanctions applicable only after the problem has occurred can be extremely costly from a social point of view. Furthermore, the supposedly high costs of uncertainty about the effects of regulation can be mitigated, even with the relatively small degree of foreknowledge that regulators can achieve[105].

AInstead of the regulator prescribing a series of regulatory commands and applying controls following a repressive logic through liability, whether civil or criminal, when damage is caused, the LGPD establishes an obligation for agents to account for the measures implemented to address possible damage and "the efficiency of the measures adopted not only to contain the risks of their activities, but also with

104 COUNCIL OF EUROPE. Guidelines on National Digital Identity. Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data. Council of Europe, February 2023. p. 12.

105 GALLE, Brian, In Praise of Ex Ante Regulation, Georgetown Law Faculty Publications and Other Works, 2015, p. 1759.

regard to compliance with data protection rules in general"[106].

Accountability, as a principle of the LGPD, has guided a logical change in the law, in which in addition to guaranteeing the right to reparation for damages when they occur, the agent responsible for processing must also act even before these damages materialize. This new logic of regulating data processing and encouraging responsible practices is a response to the greater discretion and freedom that processing agents have to process data, since the law is not prescriptive about what should or should not be done.

In rules such as the Marco Civil da Internet (art. 7, VII and IX), the legislator pointed to a context in which the data subject was responsible for deciding whether or not their personal data could be processed. However, the LGPD has progressively shared the decision-making power on the possibility and form of data processing with the processing agents, and it is up to them to choose the methods to effectively comply with the legislation. This evolution allows processing agents to adapt their data protection practices according to their specific needs, as long as they comply with the law's objectives.

The lack of a statute of limitations on the actions of the agents responsible guarantees greater freedom in their processing activities, including in the construction of digital solutions in a DPI, and, in return, these agents have more responsibility to ensure that the processing is appropriate, i.e. does not violate the rights of data subjects. In order to achieve this goal, the agent must adopt mitigation measures that prevent the occurrence of harm to individuals and these measures must be effective, which means that the agent has the argumentative burden of demonstrating that the instruments it has implemented are sufficient to minimize the mapped risks.

These measures are identified by Bruno Bioni as a precautionary machinery, which has been polished by the LGPD to describe the basic instruments for this accountability system, which is made up of the following elements[107]:

---

106 BIONI, Bruno Ricardo. Accountability no desenho (design) da regulação de dados pessoais: virtudes e vicissitudes. 2021. Tese (Doutorado em Direito Comercial) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021. doi:10.11606/T.2.2021.tde-25102022-123810. Acesso em: 2025-01-26. Resumo.

107 BIONI, Bruno Ricardo. Accountability no desenho (design) da regulação de dados pessoais: virtudes e vicissitudes. 2021. Tese (Doutorado em Direito Comercial) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021. doi:10.11606/T.2.2021.tde-25102022-123810. Acesso em: 2025-01-26. p. 66.

- ☐ Obligation for data controllers to keep a record of the personal data processing activities they carry out (art. 37);

- ☐ Obligation for data controllers to appoint a personal data controller (art. 41);

- ☐ Obligation for data controllers to draw up a personal data protection impact report as documentation of the risk management process (art. 38);

- ☐ Obligation for data controllers to implement, from the product or service design phase to its execution, measures to protect personal data from any form of inappropriate or unlawful processing (art. 46, §2);

- ☐ Obligation for agents responsible for data processing to adopt good practices so that the organization comprehensively and procedurally complies with the provisions of the LGPD (art. 50).

In DPI context, this logic of accountability has the effect of obliging the treatment agent to act before the damage occurs by mapping the impact of the infrastructure on guaranteeing people's rights and outlining practices that address this impact. This action is also a way for the actors involved in the construction of a DPI to assume their responsibilities as the developers and operators of the DPI, even if it is an infrastructure made up of a complex network of agents, whether public or private.

As indicated in the previous section, accountability reinforces the duty of agents to act in compliance with the principles of data protection, in addition to indicating a legal hypothesis that supports and justifies the processing and the tools for realizing the rights of data subjects. By complying with these obligations, the DPI's public value is unlocked and is met to the extent that data protection procedures are implemented.

Like the adoption of data provision measures, DPI development is a continuous and dynamic process, not a finite or static task in time. DPIs operate in a constantly evolving technological and social environment. People's needs, security threats, technological innovations and expectations in terms of essential services available in the digital environment are constantly changing. It is therefore crucial that the development and maintenance of DPIs be seen as an iterative and adaptive process.

In turn, the logic of accountability must accompany this dynamic nature of DPIs. Accountability measures cannot simply be implemented once and then forgotten

about. They need to be continually evaluated, updated and improved to ensure they remain effective and relevant in the face of changing technologies, public policies and social expectations.

Furthermore, the very understanding of what constitutes effective accountability or DPI application can evolve over time. Therefore, constant updates in accountability practices are required. Both the development of DPIs and the associated accountability measures should be seen as continuous processes of learning, adaptation and improvement. This requires a flexible and responsive approach, capable of incorporating feedback, lessons learned and new perspectives over time, thus ensuring that DPIs continue to effectively serve the public interest.

One of the consequences of this movement towards accountability and ensuring its effectiveness is the establishment of a public forum for scrutinizing and debating risk mapping and possible mitigation measures. The duty of accountability has the effect of obliging the data controller to generate knowledge about the possible adverse effects of an activity and, with this, to debate what measures should be adopted not only before, but also during and after a data processing activity[108].

It is worth noting the two faces of accountability, one (i) preventive, which seeks to "avoid damage or curb a risk that seems certain or confirmed[109], measurable, and the other (ii) precautionary, which is concerned with abstract risks that are not known or perceived before they occur[110]. It is up to the treatment agent to observe these two sides, which complement each other, in order to implement a broad vision of accountability, not just limited to the formal and mechanical fulfillment of compliance actions that have already been mapped out. Precautionary accountability must "qualitatively trigger a process of contestation and co-deliberation regarding the final design of its data processing activity"[111].

---

108 BIONI, Bruno Ricardo. Accountability no desenho (design) da regulação de dados pessoais: virtudes e vicissitudes. 2021. Tese (Doutorado em Direito Comercial) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021. doi:10.11606/T.2.2021.tde-25102022-123810. Acesso em: 2025-01-26. p. 225.

109 HARTMANN, O princípio da precaução e a sua aplicação no direito do consumidor. Direito & Justiça v. 38, n. 2, p. 156-182, jul./dez. 2012. p.157

110 HARTMANN, O princípio da precaução e a sua aplicação no direito do consumidor. Direito & Justiça v. 38, n. 2, p. 156-182, jul./dez. 2012. p.157

111 BIONI, Bruno Ricardo. Accountability no desenho (design) da regulação de dados pessoais: virtudes e vicissitudes. 2021. Tese (Doutorado em Direito Comercial) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021. doi:10.11606/T.2.2021.tde-25102022-123810. Acesso em: 2025-01-26. p. 229.

Hypothetical example

Weights and balances of prevention and precaution in DPI

State A implemented a digital identity system called "ID-Seguro". This identity solution allowed a person to request their digital identity through a state application and, after collecting biographic and biometric data, the person could access state and private public services online, so that the ID-Seguro functioned as a digital access key.

Prior to the launch, the team developed robust security policies, implemented end-to-end encryption, contracted external security audits, extensively trained staff in data protection practices, and carried out a detailed data protection impact assessment (DPA).

All these processes and documentation were kept internal, shared only with regulatory authorities when requested. The general public had no access to this information or opportunity to contribute to the development of the system.

State B, neighboring State A, seeing the development of ID-Seguro, decided to develop a similar system. During the process, State B published preliminary versions of the DPIA for public consultation, held public hearings to discuss the design of the system, created an advisory committee with civil society representatives, implemented an opt-out mechanism for certain functionalities after public feedback, and established a transparency portal where citizens can follow the development and use of the system.

Although State B has carried out fewer quantitative prevention actions, its qualitative approach to precaution has allowed for greater public scrutiny and adjustments based on citizen feedback.

As a result, when a security vulnerability was discovered in both systems, State A, despite its preventative measures, faced greater public resistance due to a lack of transparency. State B, on the other hand, was able to respond more quickly and with greater public support, as it had already established channels of communication and trust with the population.

> The main idea is that a precautionary accountability approach, which involves transparency and public participation, can be more effective in building trust and resilience in DPI, even if quantitatively fewer actions can be taken compared to a purely preventive approach[112].

It is in this sense that the duties of accountability, in addition to the obligations of transparency and access to data, also strengthen effective damage prevention measures and public scrutiny as a way of balancing the freedom and discretion of the agents responsible for processing personal data. The duties of accountability are not restricted to the merely artificial, bureaucratic and formal preparation of documents that indicate the link between DPI applications and data protection obligations, but encompass effective actions to minimize the risks that arise from the processing of personal data in DPI.

In this way, together with preventive accountability mechanisms, participation tools can also help to promote a **fair flow of data**. In the context of DPI as identity, personal data protection guidelines emerge as useful tools in the development and implementation of identity systems, avoiding the retention of unnecessary data and ensuring secure and non-abusive data sharing.

Drawing up a report or impact assessment is a fundamental process for mapping risks and addressing them through safeguard measures, as advocated above. As such, the construction of this document is linked to the level of contingency of the decision-making power to unblock the information flow concluded from the definition of the residual risk in the treatment[113]. It is precisely because of the agent's freedom to process data that the DPIA emerges as a regulatory strategy to make it clear how the interests in the processing of data that is the subject of the report are being balanced with the interests of the data subjects.

The impact report is both a mechanism for preventing mappable harm and a

---

112 BIONI, Bruno Ricardo. Accountability no desenho (design) da regulação de dados pessoais: virtudes e vicissitudes. 2021. Tese (Doutorado em Direito Comercial) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021. doi:10.11606/T.2.2021.tde-25102022-123810. Acesso em: 2025-01-26. p. 228.

113 BIONI, Bruno Ricardo. Accountability no desenho (design) da regulação de dados pessoais: virtudes e vicissitudes. 2021. Tese (Doutorado em Direito Comercial) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021. doi:10.11606/T.2.2021.tde-25102022-123810. Acesso em: 2025-01-26. p. 110.

space for precaution through public participation and scrutiny[114]. Therefore, since the processing agents have more freedom to process data, the following elements should be considered in an impact assessment[115]:

- The DPIA must be drawn up before the treatment is implemented, so that the possible risks associated with this treatment can be assessed beforehand and the processing can begin with the lowest possible risk.

- For each new activity or process that arises, it is necessary to assess the risks and map the personal data involved in order to verify whether or not it is necessary to draw up a DPIA, as well as to update the register of processing operations.

- The GDPR must contain a description of the (i) types of personal data processed, (ii) processing operations, (iii) purposes (including legitimate interests) and (iv) legal assumptions, as well as an (v) assessment of the necessity and proportionality of the processing operations, the risks to the rights and freedoms of data subjects and (vi) the measures to be taken to minimize those risks.

- When there are divergences in the decision-making process on risks and mitigation measures, the ANPD recommends, as a good practice, recording the different opinions identified in the process of drawing up the DPIA, including the justifications for the option adopted.

- The DPIA is a constantly evolving document, not least because the risks of a given procedure can be mitigated by adopting additional measures.

Given the peculiarities and centrality of personal data in identity systems, drawing up and updating the DPIA related to data processing is one of the tools for ensuring procedural fairness in the use of this data. In this sense, the Alan Turing

---

114 GOMES, Maria Cecília O. Para além de uma "obrigação legal": o que a metodologia de benefícios e riscos nos ensina sobre o relatório de impacto à proteção de dados. In Direito Digital: Debates Contemporâneos, orgs. LIMA, Ana Paula. HISSA, Carmina. SALDANHA, Paloma Mendes. São Paulo: Revista dos Tribunais, 2019, pp 141-153.

115 ANPD. Relatório de Impacto à Proteção de Dados Pessoais (RIPD). 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 17 jan. 2025.

Institute has developed a specific impact report model for the identity context, in which there is constant analysis of proportionality and necessity in processing, in addition to the intense flow of data[116]. Specifically, the institute's model mentions the following topics for attention:

- The boundaries of the report should be clearly delineated, specifying which components, processes and data flows are included in the scope of the report. When defining the scope, it is important to consider the entire life-cycle of the digital identity application, from initial registration and authentication to ongoing management and eventual decommissioning. This can include elements such as identity proofing mechanisms, credential issuing processes, authentication protocols, access control systems and data sharing agreements with third parties. Organizations should also take into account any supporting infrastructure, such as databases, APIs or cloud services that play a role in the digital identity ecosystem.

- All types of personal data collected, processed or stored by the system must be mapped. For each processing category, a detailed description of the specific data elements collected and their purpose in the system should be described. This inventory is essential for understanding the scope and sensitivity of the information processed by the system. By dividing the data into specific categories, such as basic personal information, contact details, government-issued identification and biometric data, it is possible to better assess the possible data protection implications associated with each type of information.

- There should be a detailed description of all the methods used to collect personal data. For each method, the process and types of data collected should be described, as well as the direct and indirect sources. This helps to identify possible risks and ensures transparency in data processing practices.

- A clear justification of why your system is necessary should be presented, considering alternatives and possible impacts. This justification should be

116 THE ALAN TURING INSTITUTE. Privacy impact assessment. Disponível em: https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.turing.ac.uk%2Fsites%2Fdefault%2Ffiles%2F2024-09%2Ftdi_privacy_impact_assessment_template.docx&wdOrigin=BROWSELINK. Acesso em: 17 out. 2024.

aligned with your stated objectives and demonstrate careful consideration of the privacy implications to answer, for example, what other solutions were explored? Why were these alternatives not chosen? How will end users directly benefit from this system? What improvements in user experience can they expect?

- The fairness and transparency mechanisms in place to ensure the secure processing of personal data should be explained, including details of privacy notices and any measures to prevent misleading or discriminatory practices. It is important to detail how to ensure that data subjects are fully informed about data processing activities. Consider all points of contact where transparency is crucial, from data collection to the exercise of data subjects' rights.

- A comprehensive overview of all third-party interactions involving personal data within a digital identity system should be provided. It is important to detail the complex network of partnerships and service providers (in identity systems), for example identity verification services, cloud storage providers, analytics platforms or government agencies. The aim is to create a clear map of where data flows, why it is shared and how it is protected along its journey.

This model is very similar to the DPIA, which makes it a relevant reference between the intersection of data protection and digital identity. These tools are fundamental for accounting for the processing of personal data, as they are key to the functioning of identity solutions in a DPI. It is through the preparation of an impact report that it is possible to map the risks to be faced by DPI users, as indicated in the following table:

Risk	Mitigation measure
Non-compliance with the separation of information and the competence of agents	All data processing must be aimed at fulfilling a specific purpose by a competent agent. In this sense, it is the purpose that directs who should process certain personal data, and it is not possible to say that an agent is competent to process the data it knows for any purpose, nor that all the entities that make up that agent can process the data that one of its parts has access to, as if it were an informational unit. Personal data must be segregated according to the purpose for which it is processed, avoiding a concentration of information, which would lead to a concentration of power. One way to avoid possible abuses in data sharing is to guide the flow of data by dividing the competencies of the agents who send and receive personal data.
Intrusive data processing	Data processing should only concern data that is necessary to achieve a certain purpose and, if there is another, less intrusive form of processing, it should be implemented. For this reason, the responsible agent must keep a record of the description of the specific problem the DPI application aims to solve, as well as the opportunities it seeks to capitalize on, the other alternatives considered and why these options were not chosen. It is also important to indicate how the end users will directly benefit from this system, what improvements in the user experience they can expect and how the system increases the efficiency or operational effectiveness of the activity that was previously fulfilled outside of DPI.
Who you send data to: inappropriate sharing. For those who receive data: irregularity in reuse.	The entire sharing process must be documented, whether sending or receiving personal data. This includes a description of the name of the third-party institution sending or receiving the data, the reason for the sharing, the data shared and the legal basis for the sharing. In addition, data may only be processed for a secondary purpose if the following criteria are met: ▪ indication of an appropriate legal basis to support the new treatment; ▪ compatibility of the secondary purpose with the purpose of data processing at the time of data collection, the primary purpose; ▪ the provision of a sufficiently specified purpose, which allows the assessment of the public interest to be achieved; ▪ compliance with the principles of data protection and the rights of data subjects, in particular the principle of transparency, necessity, adequacy and accountability and the right to information and access.

Person as an object of identification and not a subject to be identified	In a probabilistic logic of identification, various pieces of data are valued as elements with some degree of relevance to identifying someone, even if this information has not been provided by the person to be identified. The person becomes a passive object of identification, without knowing what information has been used to form their identity. Based on this probability of being who they say they are or participating in a specific group, the person is profiled based on statistical inferences and data correlations, rather than certainties about a person's identity or characteristics. This digital version of the person is sufficient for them to be able to access certain essential goods or services, even if only to a limited extent, putting the people being identified at risk. Therefore, secure profiling models must be implemented, audit trails to ensure that decisions are reasonable and appropriate, as well as regular ongoing review of profiling algorithms to avoid bias, and human supervision and review.
Imbalance of power in the lack of information about the data processing that the person is subjected to and in the lack of mechanisms to meet the rights of data subjects	The lack of knowledge about data processing and DPI, in general, prevents users from objecting, questioning and knowing how their data is being processed, which increases an imbalance of power between users and the agents responsible for DPI. In the absence of instruments for users to report problems with the DPI and demand that their rights as data subjects be enforced, a module that allows faults to be addressed and held accountable must be added to the DPI, otherwise a context of disapproval and distrust in its operation will be created.

The identification of risks for the user goes beyond the risks of information security or access to intimate information in a logic of secrecy[117]. These risks are not the subject of a DPIA, since it aims to understand the risk to the rights and freedoms of data subjects. Further contextualization and in-depth analysis is required to indicate the risks pertinent to a DPIA, as indicated in the table above.

The procedure for drawing up the impact report is fundamental, insofar as not only the outcome of the process is relevant to defining whether the treatment should continue or not and whether the measures are sufficient to minimize the perceived risks. The way in which these results are articulated has an impact on the very validity and legitimacy of the report, which starts to look at the treatment from several different and complementary perspectives. To guarantee this legitimacy, two models are interesting from a regulatory point of view[118]:

117 Dessa forma, o modelo de RIPD desenvolvido pela SGD apresenta uma estrutura de descrição da atividade de tratamento relevante para contextualização do tema, mas, quando exemplificando os riscos ao tratamento de dados, o modelo indica o tratamento de dados sem o consentimento do titular como um risco, bem como o compartilhamento de dados com terceiros sem o consentimento do titular e a perda ou roubo dos dados. SGD. Framework, Guias e Modelos do Programa de Privacidade e Segurança da Informação (PPSI). https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_template_ripd.docx. Acesso em: 06 fev. 2025

118 BIONI, Bruno Ricardo. Accountability no desenho (design) da regulação de dados pessoais: virtudes e vicissitudes. 2021. Tese (Doutorado em Direito Comercial) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021. doi:10.11606/T.2.2021.tde-25102022-123810. Acesso em: 2025-01-26. p. 112.

DPIA as an accountability tool[119]		
Measure	Publication of the DPIA in a space accessible to interested parties	Involvement of stakeholders in drawing up the DPIA
Purpose	Public scrutiny of the value judgment of why a data processing activity is considered low, medium or high risk.	Participation in defining the methodology by which risk management will be implemented. Opportunity for stakeholders to have a say from the outset and not just at the end.
Effect of not implementing the measure	DPIA would be an instrument to reinforce the asymmetry of information between the agent who carries out the treatment activity and the people subjected to it.	DPIA would be a bureaucratic and neutral document, with no room for review and questioning by stakeholders.
Disadvantages of implementing the measure	Stakeholders could only access the results of the DPIA, with no room for effective dialog.	Organization of formal and fixed spaces for the involvement of all stakeholders

As a result, the process of the agent responsible for processing demonstrating that it has adopted effective measures capable of proving compliance with data protection rules is not a monologue in which only that agent has a place to speak. Ensuring the meaningful participation of affected people and groups should be a prerequisite for a process that seeks to assess impacts on human rights. Through participation mechanisms, rights-subjects can access information and better understand the project and the resulting impacts, but also learn about their rights and the respective responsibilities of the treatment agents. If done carefully, participation can be a way of empowering rights subjects[120].

119 GOMES, Maria Cecília O. Para além de uma "obrigação legal": o que a metodologia de benefícios e riscos nos ensina sobre o relatório de impacto à proteção de dados. In Direito Digital: Debates Contemporâneos, orgs. LIMA, Ana Paula. HISSA, Carmina. SALDANHA, Paloma Mendes. São Paulo: Revista dos Tribunais, 2019, pp 141-153.

120 THE DANISH INSTITUTE FOR HUMAN RIGHTS. Crosscutting: Stakeholder engagement human rights impact assessment guidance and toolbox. 2020. Disponível em: https://www.humanrights.dk/files/media/document/HRIA%20Toolbox_Stakeholder%20Engagement_ENG_2020.pdf. Acesso em: 17 jan. 2025.

The DPI, as an instrument of accountability, must be built in dialog with the agents impacted by the processing activity, especially in DPI solutions, which, by definition, will reach a large part of the society that uses it, causing large-scale data processing.

For the ANPD, the publication of the DPIA is not mandatory, but it recognizes that "allowing access to the general public can be a measure that demonstrates the controller's concern for the security of the personal data under its responsibility and its commitment to the privacy of the data subjects, in addition to complying with the principles of free access, transparency and responsibility and accountability"[121]. The publication of the DPIA is a way of complying with the fundamentals of the LGPD by making it clear which agents are responsible for the processing, whether they are persons governed by public or private law, as well as the risks identified and the mitigation measures implemented to address these risks, making it possible for those affected to know in advance the parameters mapped out by the controller.

At the same time, in relation to public entities, the authority states that "the DPIA must be published: (i) by order of the ANPD, under the terms of art. 32 of the LGPD; or (ii) by the controller itself, when no hypothesis of secrecy applicable to the case is identified, in accordance with Law No. 12,527, of November 18, 2011"[122], the Access to Information Law (LAI). The LAI aims to guarantee the publicity of information processed by the government, and also applies to private non-profit organizations that receive public funds directly from the budget or through social grants, management contracts, partnership agreements, covenants, agreements, adjustments or other similar instruments to carry out actions in the public interest. Consequently, when there is no hypothesis of secrecy that applies to the publication of the DPIA, the private entity that is subject to the LAI must also publish the report.

Accountability serves as a mechanism for control and continuous improvement of the DPI. By requiring processing agents to prove compliance with data protection principles and the rights of data subjects, it ensures that the public interest is

121 ANPD. Relatório de Impacto à Proteção de Dados Pessoais (RIPD). 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 17 jan. 2025.

122 ANPD. Relatório de Impacto à Proteção de Dados Pessoais (RIPD). 2023. Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/relatorio-de-impacto-a-protecao-de-dados-pessoais-ripd. Acesso em: 17 jan. 2025.

effectively served. Furthermore, the notion of accountability also ensures that the use of personal data in DPI is transparent and justifiable to society. This is crucial to maintaining public trust in the institutions and digital services offered.

4.2.2. Accountability through participation procedures

Defining and promoting public value in a DPI presupposes an inclusive and participatory process. As argued in this report, DPI must be oriented towards serving the interests not only of private agents, but also the common good of the society that uses it. This common good, this public value, should not be perceived as an abstract concept defined by specialists or public managers, but as a **collective construction that emerges from the interaction** between different sectors and social groups. Understanding public value means recognizing the diversity of perspectives, needs and aspirations of the groups that make up a community.

Promoting public value is a prerequisite for any DPI, as presented in the previous sections. In this sense, the effective participation of society in the development of digital infrastructures is fundamental to ensuring that technological solutions genuinely respond to collective desires. By enabling co-creation spaces, communities can actively influence the design, implementation and monitoring of these infrastructures. As a result, this collaborative approach makes it possible to create tools that not only solve immediate problems, but promote social transformation, innovation and inclusive growth.

Knowing that DPI and its applications must serve the public interest, social participation practices become **tools** to ensure that society's interests and demands are being addressed, whether before, during or after the implementation of DPI.

The common good emerges precisely from this collective construction, where different sectors dialog to define priorities and strategies for DPI. Digital public infrastructures are then understood not as neutral instruments, but as living spaces for social transformation, whose value materializes in their ability to respond to the specific needs of each community. Public value is thus constituted as a **dynamic process** of learning and permanent collaboration.

Civic participation ensures that this infrastructure is developed in line with the population's expectations. Through community involvement, it is possible to prioritize

digital services that are most urgent or relevant to people's daily lives. In addition, different regions or social groups may have specific needs that need to be considered when implementing DPI, promoting a more inclusive approach adapted to the local context.

Citizen participation is not only a democratic requirement, but also a fundamental requirement for the **efficiency of** digital policies[123]. When adopted throughout the life cycle of these policies, participatory governance can reduce the risks created by the system, accelerate innovation with creative solutions to concrete demands and increase the acceptance and continued use of DPI applications.

Participation is one of the key tools for identifying gaps and potential risks before they become real problems. Citizens from different backgrounds and experiences, as well as representatives of other sectors and interests, can offer diverse perspectives, pointing out challenges that developers and public managers may not have foreseen.

This interaction with other agents to map gaps in the DPI can result in benefits, including economic ones, by **minimizing cases of rework**[124]. In a scenario without the participation of various actors in the DPI, after the application has been developed, it is likely that it would have to be revised due to a flaw or column that was easily noticed by other actors at an earlier time.

For there to be participation in the construction of public value, it is essential to consolidate **formal mechanisms** that allow plural participation. It's not enough to create occasional and symbolic consultation channels; it's necessary to set up deliberation processes in which different groups can share their perspectives, contribute their knowledge and participate in decisions. The formalization of these moments of participation are essential to guarantee parity and predictability in the interaction of sectors, ensuring that everyone can effectively influence the DPI's decision-making process.

---

123 LUCIANO, Maria. Digital Public Services for Whom? Participation and Care as Prerequisites for Efficiency. 2024. Disponível em: https://www.techpolicy.press/digital-public-services-for-whom-participation-and-care-as-prerequisites-for-efficiency/. Acesso em: 25 jan. 2025.

124 TENNISON, Jeni. Mechanisms for Governance Cooperation Why We Need Inclusive Data Governance in the Age of AI. 2024. Disponível em: https://www.cigionline.org/articles/why-we-need-inclusive-data-governance-in-the-age-of-ai/. Acesso em: 2 dez. 2024.

One of the formal mechanisms for participation used by public authorities are **public consultations** in which interested groups sign up to debate a preliminary version of the rule. With the amendment of the Law on the Introduction of the Norms of Brazilian Law by Law 13.655[125], public consultation gained prominence as one of the stages to be implemented by public bodies when issuing normative acts. Article 29 of this law states that "in any body or power, the issuing of normative acts by an administrative authority, except those of mere internal organization, may be preceded by public consultation for the manifestation of interested parties, preferably by electronic means, which will be considered in the decision".

The aim is to ensure that interested parties have the opportunity to express their views and that their comments are taken into account in the agency's final decision. To this end, it is essential that the information and reports on which the consultation is based are made available, so that participation is informed, and that there are responses to the "contributions sent, motivating the incorporation or not of the suggestions in the final version of the act [...] and publicizing its reasons regarding the final content"[126]. This hearing can be held at any time during the construction of the standard, whether before or even after publication, bearing in mind the challenges and particularities that arise during the implementation of the standard.

Society's participation also has the potential to guarantee greater legitimacy for DPI by listening to the people concerned. As a necessary measure for conducting DPI-related processes, consultation would not just be a rhetorical tool, it would allow people to actually influence the decision-making process. This collaborative dynamic allows technologies to be truly people-centered, reflecting social diversity and complexity.

With regard to the element of participation in the DPI, Article 16 of Decree 12.069/2024 states that the Digital Government Secretariat must promote the development, implementation and use of the DPI, in conjunction with other agents, including those external to the Government, such as representatives of society, the academic sector and the private sector. The federal government itself recog-

125 https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13655.htm

126 LIMA, Gabriel; GASPAR, Luciana. As Consultas Públicas Enquanto Mecanismo de Legitimação dos Atos Administrativos. Revista Opinião Jurídica, v. 20, n. 34, p. 1-29, 2022. Disponível em: https://www.redalyc.org/journal/6338/633875004001/html/. Acesso em: 2 dez. 2024.

nizes that DPI and its applications must be built in **dialogue** with various agents beyond the Public Power.

In addition to public consultations, this dialog can be built up through the formation of multi-sectoral committees set up to establish standards and guidelines for DPI. The provision of committees as a deliberative space on activities carried out by public authorities that affect society is common and one of the ways to ensure openness and participation in public activities. As an example, Law 13.444/2017, which provides for National Civil Identification (ICN), established the program's Management Committee, Decree 10.046/2019 created the Central Data Governance Committee (CCGD), and the LGPD provided for the National Council for the Protection of Personal Data and Privacy (CNPD), made up of representatives from various sectors, as a space for oxygenating other areas in the public debate.

It is worth noting that not just any type of council meets the democratic principles and values of participation. The STF, in the judgment of **ADI 6649**, a case already discussed in this report, declared the composition of the CCGD provided for in article 22 of Decree 10.046/2019 unconstitutional. The court found that the criteria for choosing the committee's members were contrary to the constitution, as they included only representatives of the federal public administration, without adequate **democratic openness**.

In the context of art. 21 of the Decree, the CCGD was responsible for deciding on rules for sharing data, guidelines and directives for integrating bodies, as well as setting up other reference base registers for the public sector. In the original structure, this Committee would only be made up of representatives of the Government, without any participation from other sectors.

In view of the Committee's powers and composition, the ADI's rapporteur argued that the Committee "not only offers deficient protection for core values of the constitutional order, but also constitutes a destabilizing factor for the guarantees provided for in Law 13.709/2018". This is because there is "a certain consensus on the need to create independent administrative authorities, specifically assigned to oversee and control activities that potentially harm the right to privacy"[127].

127 SUPREMO TRIBUNAL FEDERAL. Ação Direta de Inconstitucionalidade 6.649 Distrito Federal. p. 57. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978491&ext=.pdf. Acesso em: 2 dez. 2024

Contrary to this consensus, the Committee would be "an institution with an **insular profile, hostile to any proposal for democratic openness and pluralization of the debate** and, to that extent, closed to the participation of representatives from other republican institutions and civil society entities"[128]. For this reason, the Committee was declared unconstitutional.

It is therefore essential to provide spaces for debate and participation on issues related to the affectation of the fundamental right to data protection, and these spaces must be independent, open and plural. The court is explicit in recognizing that the "effective protection of the right to privacy depends on the correct calibration of the institutional profile of the bodies responsible for regulating, controlling and monitoring personal data processing activities"[129].

In this sense, it is worth noting that, in order to guarantee a fundamental right to the protection of personal data, it is necessary to consider the close link between fundamental rights, organization and procedure, in the sense that fundamental rights are, at the same time and to a certain extent, dependent on organization and procedure [...], but simultaneously also act on procedural law and organizational structures"[130]. The provision of deliberative councils on data processing activities is fundamental to **preserving the fundamental right to data protection**, and these spaces must be independent, participatory and plural.

In view of the STF's decision in ADI 6649, the CCGD is currently made up of various bodies from the three branches of government, such as the Civil House, CGU, MJ, Bacen, CNJ, Senate and Chamber of Deputies, as well as two members of civil society[131]. In 2020, the CCGD set up the Data Governance Technical Subcommittee with the power to propose guidelines for structuring the Data Governance of the bodies and entities of the direct, autarchic and foundational federal public admin-

---

128 SUPREMO TRIBUNAL FEDERAL. Ação Direta de Inconstitucionalidade 6.649 Distrito Federal. p. 61. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978491&ext=.pdf. Acesso em: 2 dez. 2024.

129 SUPREMO TRIBUNAL FEDERAL. Ação Direta de Inconstitucionalidade 6.649 Distrito Federal. p. 60. Disponível em: https://portal.stf.jus.br/processos/downloadPeca.asp?id=15358978491&ext=.pdf. Acesso em: 2 dez. 2024.

130 INGO SARLET. Proteção de dados pessoais e deveres de proteção estatais. Consultor Jurídico. Disponível em: https://www.conjur.com.br/2021-ago-27/direitos-fundamentais-protecao-dados-pessoais-deveres-protecao-estatais/. Acesso em: 2 dez. 2024.

131 MGI. Comitê Central de Governança de Dados (CCGD). 2020. Disponível em: https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadedados/comite-central-de-governanca-de-dados. Acesso em: 2 dez. 2024.

istration and the other Powers of the Union[132]. This assignment directly impacts how possible DPI architectures can be structured to promote or restrict the flow of data, including personal data.

The CCGD's attributions are close to issues of governance and the flow of data, including personal data. However, it is possible to argue that its composition is not representative enough to address the interests of the groups affected by a DPI, since it is mostly made up of executive branch bodies, with eight members, as well as two members from civil society and four invited members from other branches of government. Knowing that public value emerges from the interaction of interested groups, in addition to public managers, the operators of the infrastructure, the recipients of its functions, and the institutions and groups affected by the DPI should be part of these councils.

In the context of public infrastructure, whether or not the CCGD is reformed, this council could be made up of players from different sectors, at least from the public sector, the three spheres of power, the private sector, the third sector and the academic community, and could also act in assessing and resolving problems related to DPI[133], promoting transparency and accountability among players, and protecting the rights and interests of users.

To be effective, the board must have the authority to analyze complaints and make recommendations, operating independently of the government and technology providers. It is important that there is independence in the way the body makes decisions, so that it is not subordinated to other structures that may have interests of their own that are not linked to the DPI's purpose. Thus, the council would be competent to:

- Propose strategic guidelines and provide subsidies for the development of a DPI;

- Prepare studies and hold debates and public hearings on DPI;

---

132 MGI. Cartilha de Governança de Dados. Disponível em: https://www.gov.br/governodigital/pt-br/infraestrutura-nacional-de-dados/governancadedados/arquivos/CartilhadeGovernancadeDadosEcossistemadeDados.pdf. Acesso em: 2 dez. 2024

133 Essa é a composição mínima de conselhos como o CGI.br e o CNPD. Disponível em: https://cgi.br/membros/ e https://www.gov.br/anpd/pt-br/cnpd-2/composicao-cnpd/estrutura-cnpd-1.

- Oversee changes and feedback from DPI users; and

- Suggest actions to be taken by the DPI agents.

It should be noted that these competencies are broader than those of the CCGD, which is limited to deliberating on data sharing between federal public administration bodies in the context of the Citizen's Base Register[134]. Furthermore, the implementation of active transparency measures in its actions and decisions could also strengthen public confidence in the council.

Participation gives the DPI greater **legitimacy**, as it is seen as a product of collective effort and not just a government imposition. The diversity of perspectives brought by participants can lead to innovative and creative solutions to complex challenges faced by society. Furthermore, a DPI developed with broad participation is more likely to be sustainable in the long term, as it has the support and understanding of the population.

The benefits of participation are anchored in tangible improvements in the DPI that they perceive in their daily lives. Whether through improved services, the development of specific infrastructure or the simplification of processes, participatory engagement and collaborative efforts are key to the success of a DPI[135]. Thus, in addition to data prevention practices, participation procedures would also function as one of the DPI's forms of accountability to society, ensuring the promotion of the common good.

Understanding accountability as a tool for realizing the public interest also implies establishing an institutional space for public proposal and deliberation. Whether through public consultations or the establishment of specific councils, participatory tools must be implemented to ensure a **collaborative normative and regulatory process[136]**.

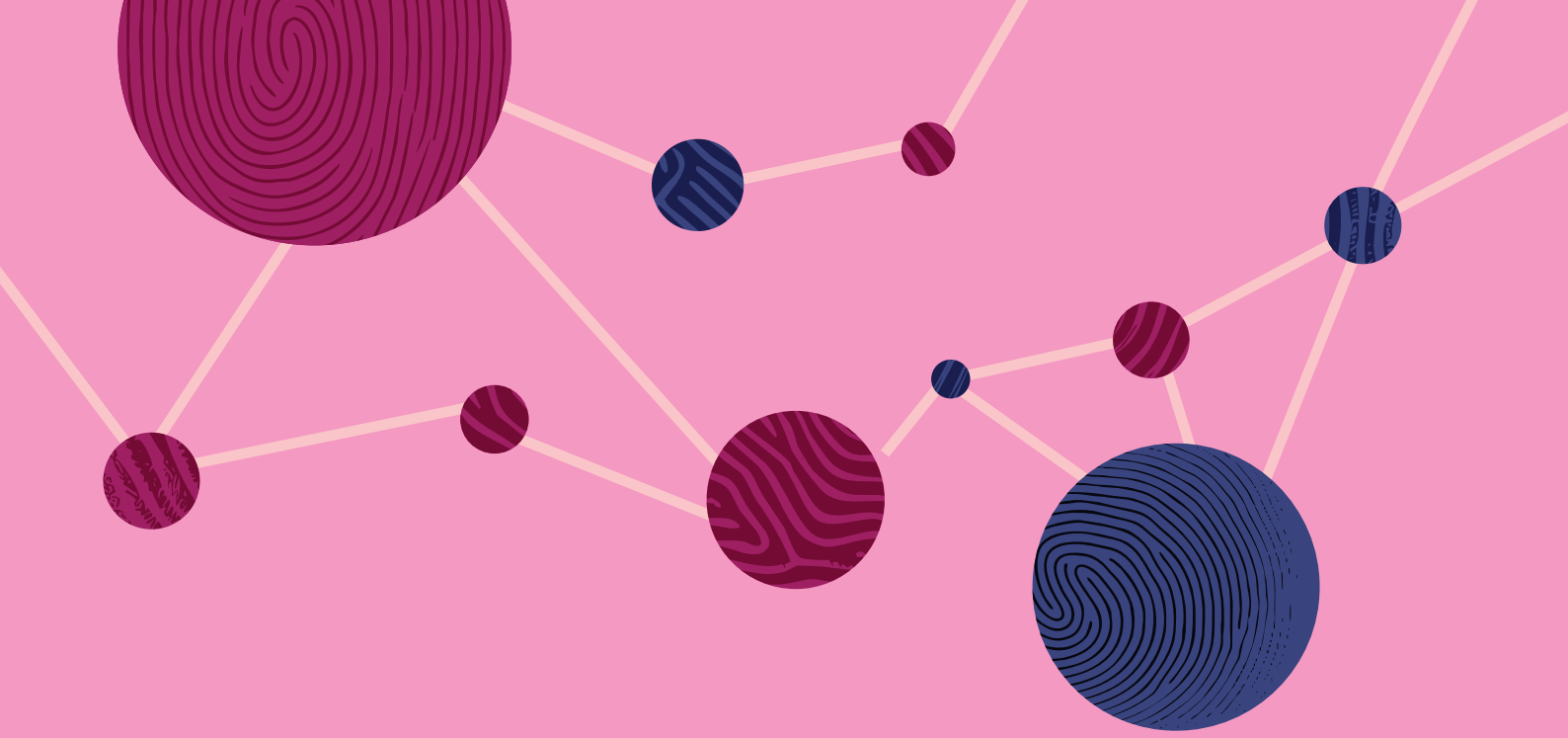
---

134 PRESIDÊNCIA DA REPÚBLICA. Decreto n 10.046, de 9 de outubro de 2019. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/decreto/d10046.htm. Acesso em: 2 dez. 2024.

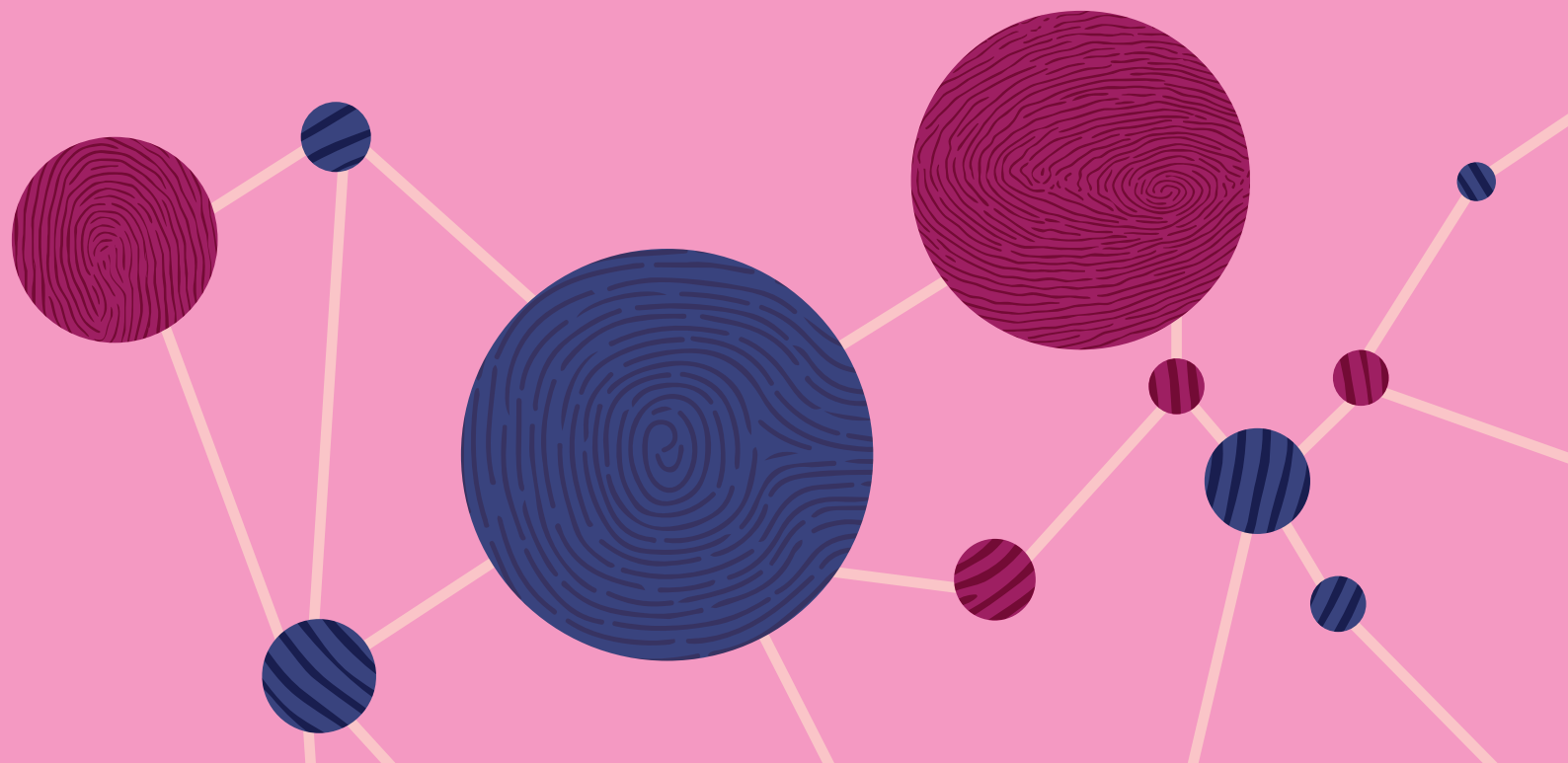
135 ODI RESEARCH. What makes participatory data initiatives successful? [s.l.: s.n.], 2024. p. 9. Disponível em: https://theodi.cdn.ngo/media/documents/What_makes_participatory_data_initiatives_successful_.pdf. Acesso em: 2 dez. 2024.

136 BIONI, Bruno Ricardo. Accountability no desenho (design) da regulação de dados pessoais: virtudes e vicissitudes. 2021. Tese (Doutorado em Direito Comercial) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2021. doi:10.11606/T.2.2021.tde-25102022-123810. Acesso em: 2025-01-26. p. 129

Thus, from a formal, plural and robust perspective, it is possible to establish guidelines for DPI to aim for the common good. An appropriate governance structure encourages the use of technology that enables collaboration between stakeholders, or even co-creation. This includes promoting innovation in line with established guidelines, adopting interoperability and structuring tools that facilitate participatory governance based on a plural understanding and geared towards the public interest.



05.
FINAL CONSIDERATIONS



5 Final considerations

The challenges and risks of implementing digital identity systems as a DPI tool are being mapped and understood as the DPI solutions are developed. It is in this sense that this report looks at the **intersection between identity, DPI and data protection,** precisely in order to identify possible tensions and areas for improvement. Based on the connections between digital identity, DPI and the Brazilian constitutional grammar of data protection, the report proposes governance measures to guarantee a fair flow of information.

To this end, the research uses interviews with experts, analysis of literature and case law, and discussion at events to understand the issues of tension and, with this, to draw up recommendations, which include the promotion of citizen participation, transparency, and the adoption of robust structures for the management of DPI and identity solutions. The report emphasizes the need to reconcile technological innovation with the protection of fundamental rights in the face of **governance** obligations **to promote public value and accountability** in the processing of this data.

Initially, the report explores the key concepts of DPI and digital identity in order to map the variables present in this context, since DPI provides the basis for the functioning of digital identity systems. DPI is the necessary infrastructure for the operation of essential systems and services in the digital environment, aimed at promoting the common good and serving a public value. It must therefore have elements of **participation, interoperability and data protection to allow new applications to be built from a common foundation aimed at serving the public interest**. Identity, as one of the applications of this DPI, must observe these founding elements.

Faced with the extensiveness of identity as DPI, the risks to fundamental rights must be perceived. With regard to the right to data protection, the report addresses the asymmetry of power between state and citizen, intensified by digitalization, and the LGPD's response in the search for a new balance. The STF's ruling on ADI No. 6387, which recognized **data protection as an autonomous right**, rightly affirms the legal protection of all personal data, regardless of its nature. In this sense, the development of DPI and identity solutions falls within this new paradigm and must comply with the constitutional right to data protection.

The concepts of informational self-determination and the free development of the personality gain relevance in this new context of personal data protection. Self-determination goes beyond consent and must guarantee the autonomy of the individual in defining their interests and needs in relation to their data. Based on these concepts, digital identity, constructed from data flowing through the digital infrastructure, can be an instrument for **distributing power** to the extent that its development ensures informational self-determination.

Theories such as privacy as contextual integrity are relevant precisely in order to establish barriers and guidelines so that data processing is in line with the data subject's expectations. According to this theory, privacy would be preserved to the extent that the **flow of data respects contextual norms**. According to Nissenbaum, five elements define these norms: social spheres of the data subject, sender and recipient, type of information and restrictions on transmission. Furthermore, in order to identify whether the data flow is appropriate or not, the interests of the parties, political and ethical values, as well as contextual purposes and values, must be considered. Thus, in the context of DPI, data sharing, including identity data, could occur if the context of the relationship between the agents involved is observed.

Furthermore, from the point of view of the **informational separation of powers**, in the context of digital constitutionalism, the state should not be an informational unit. This means that the sharing of data between public bodies and entities must respect their powers to process the specific data of specific data subjects. In this sense, the decisions in ADI nº 6529/DF, ADPF nº 692/DF and MS nº 36.150/DF consolidated the understanding that **data sharing must be motivated, meet the public interest, respect the reservation of jurisdiction and observe the principles of the LGPD.**

The Brazilian constitutional grammar of data protection plays a fundamental role in the development of identity applications in DPI. It is therefore essential that these parameters, already consolidated in Brazilian jurisprudence, are taken into account to guide the development of this infrastructure.

The preservation of the common good in DPI is intrinsically linked to the guarantee of the fundamental right to the protection of personal data. Public value is not just about generating economic value from data, but requires a fair and equitable distribution of the benefits, with respect for individual rights. As a result, the object of

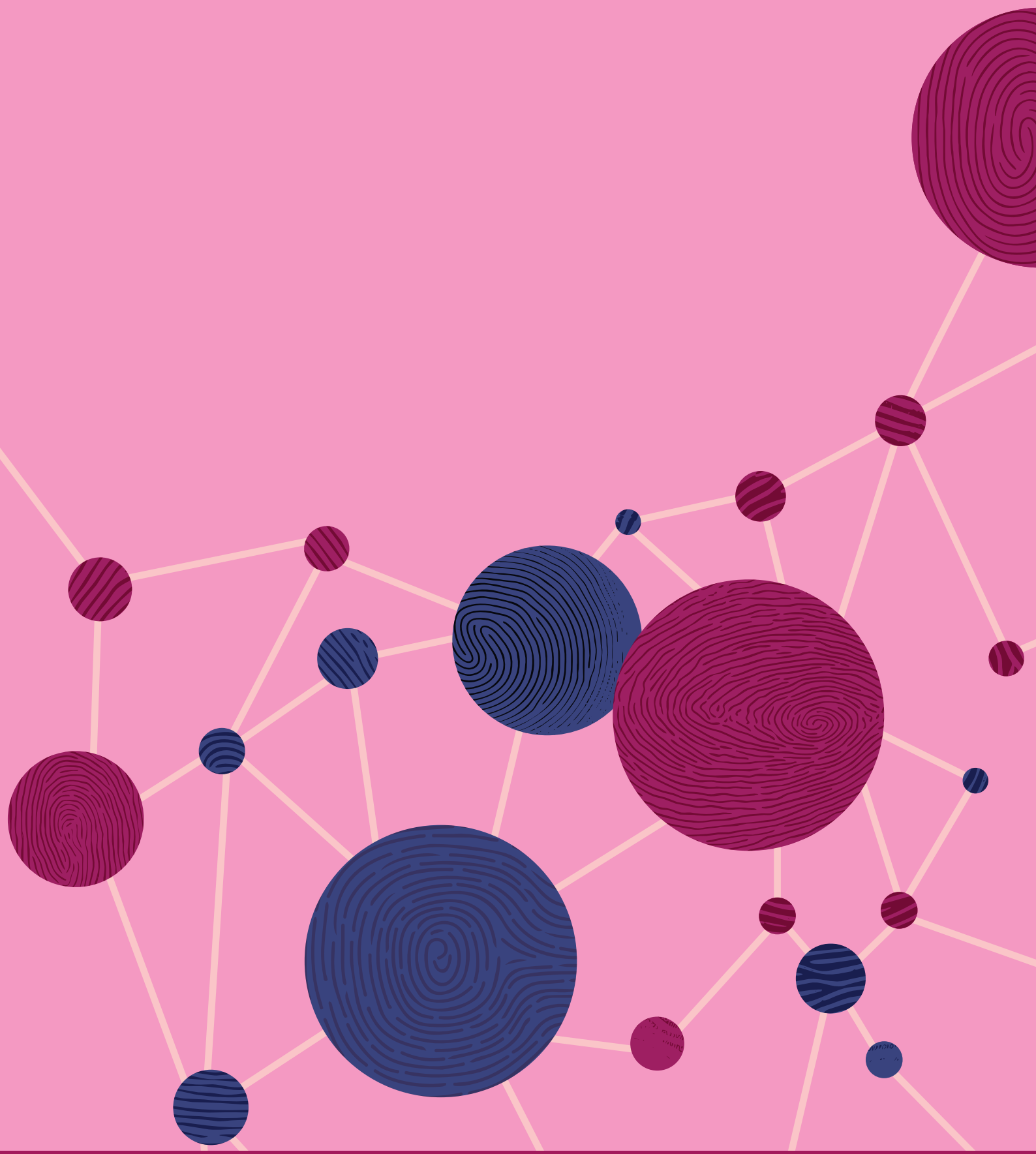
protection is not just secrecy, but the safe and appropriate circulation of personal data. This data protection, as established by the STF, also promotes the public interest, and the legal obligations of the LGPD instrumentalize this promotion with legal certainty.

In order to guarantee this protection, it is essential to define areas of responsibility and accountability mechanisms. Users must have mechanisms to compensate for damage suffered, with clear responsibilities for each agent. Trust in the infrastructure depends on the robust definition of levels of responsibility. For this reason, the information flow must be mapped and aligned with data protection parameters to guarantee the public interest and compliance with other data protection parameters.

The regulatory logic of data protection also implies the implementation of accountability obligations based on a preventive rationale, with the aim of protecting data subjects before damage occurs, rather than only applying sanctions a posteriori. The actors involved in DPI must demonstrate responsibility by being accountable for the measures implemented to mitigate potential damage and ensure compliance with data protection regulations. This responsibility is driven by the greater freedom these agents have when building digital solutions within the DPI. Thus, the drafting of the DPIA, as well as the implementation of participatory practices and public scrutiny are encouraged as a way of balancing the freedom and discretion of the agents responsible for processing personal data.

For identity systems to be considered DPI applications, it is essential that they maximize the public good and are governable, participatory systems that allow for improvement based on the responsibility of the agents involved. In a context of layered identity, transparent, accountable and collective processes are essential if an identity is to be a tool for accessing the infrastructure and its applications.

In conclusion, the importance of a proactive approach to data protection in the development of DPI and digital identity, using Brazilian constitutional grammar as a basis, is highlighted. In line with STF rulings, **the concepts of data protection and public interest are not antagonistic; on the contrary, they must be balanced, given that the public interest is realized in the effective guarantee of the protection of personal data**. In this sense, identifying the common interest, accountability tools and the social participation of various agents are crucial to guaranteeing a fair flow of information, protecting fundamental rights and promoting public value.



DataPrivacyBR Research

SUPPORTED BY:

ripple