THE INFRASTRUCTURE OF IDENTITY: THE INFLUXES OF A DIGITAL IDENTITY AS AN APPLICATION OF DPI

Eduarda Costa Almeida
Pedro Bastos Lobo Martins

DataPrivacyBR Research

APOIO
ripple

About us

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.

DIRECTORS

Bruno Bioni, Mariana Rielli and Rafael Zanatta

COORDINATORS

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

TEAM

Alicia Lobato, Eduarda Costa, Eduardo Mendonça, Gabriela Vergili, Horrara Moreira, Isabela Gomes, Isabelle Santos, Johanna Monagreda, João Paulo Vicente, Júlia Mendonça, Louise Karczeski, Matheus Arcanjo, Mekebib Assefa, Nathan Paschoalini, Otávio Almeida, Pedro Henrique, Rafael Guimarães, Rafael Regatieri, Roberto Junior, Rodolfo Rodrigues and Vinicius Silva.

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. The infrastructure of Identity: The influxes of a digital identity as an application of DPI. São Paulo: Data Privacy Brasil Research Association, 2024.

Executive Summary

There is a growing demand for the development of a digital public infrastructure (DPI) to promote access to essential rights and services for people, just like physical infrastructure. There is a significant effort in international debates to outline the shape of a DPI, as well as its concept and applications. In addition, it is essential to realize that the elements of open and interoperable technology, with robust governance and multisectoral participation are essential to guarantee the trust, transparency and accountability of the infrastructure, as well as promoting inclusion and innovation..

Although the definition of DPI is still evolving, it is important to recognize that applications of this infrastructure must **serve the common good** and **maximize public value**. The element of public value is added to other essential elements to characterize an application as DPI. DPI applications are constituted as such in a process of constant updating, and not just on the basis of a fixed classification which considers the application as part of a DPI ecosystem or not.

One of the key structural elements of DPI is the **active engagement of various sectors of society in the development and governance of DPI.** This engagement is crucial for fostering innovation and creating user-centered solutions, particularly in areas such as identity. Nonetheless, for this multisectoral engagement to be impactful, it requires the definition of formal and material standards through which society can shape the evolution of DPI applications, their execution, and oversight.

One of the main materializations of DPI is the identity applications. This is due to the fact that a digital infrastructure is only effective and gains practical significance when it enables the identification of application beneficiaries in a secure and convenient manner. As infrastructure becomes digitalized, identity validation procedures are crucial for individuals to **access** rights, public or private products or services.

In this perspective, digital identity works as a set of unique electronic attributes that perform certain functions, such as guaranteeing the reliability of a person's credential, with the potential to simplify this identification process. In general, these systems must perform the basic functions of identification, authentication and authorization, forming an essential cycle to guarantee their usefulness.

In addition to conventional functions, these systems can involve a **few or several actors** with specific roles, such as identity providers, system operators and trust entities. These actors can organize identity systems in **centralized, federated or**

decentralized structures, which influences the management of these systems. In addition, identity systems can have **foundational** purposes, seeking to provide a legally recognized universal identity, or **functional** purposes, issuing credentials to authorize specific access, or even other purposes depending on the context in which the identity is validated.

With the complexification of identity systems and the combination of these frameworks, **layer-based identity models** are becoming more popular as DPI applications. These models are the result of the integration of multiple digital systems made up of different sources and contexts, which tension the **purpose** of data collection with the compatibility of subsequent uses.

Identity systems in a DPI present **specific risks** for people's autonomy and personality development that go beyond the sum of the risks of an identity system and its digitization considered in isolation. Constant and uninformed monitoring of people's behavior and attributes can restrict the autonomy and free development of those identified.

Thus, sharing identification information from different contexts can lead to serious violations of privacy rights, given the lack of **informational separation** between the agents involved. Furthermore, it is possible that the risks generated in one identification context (e.g. fraud detection) may manifest themselves in other contexts (e.g. when applying for a job), due to the flow of data.

In view of these risks, identity systems must:

- Implement data protection as a fundamental principle, requiring the adoption of transparency approaches, establishment of purpose and specific data sharing rules, always seeking to minimize data sharing;
- Seek approaches that prioritize people's power of agency, always guaranteeing the right to explanation and review of decisions made about them;
- Prevent the aggregation of data in a single centralized database or the retention of unnecessary data, limiting the collection and use of personal data to protect people from data misuse;
- Introduce robust mechanisms to ensure that the sharing of attributes and credentials takes place in a secure and traceable manner, and that data is accurate, complete, kept up-to-date and relevant;

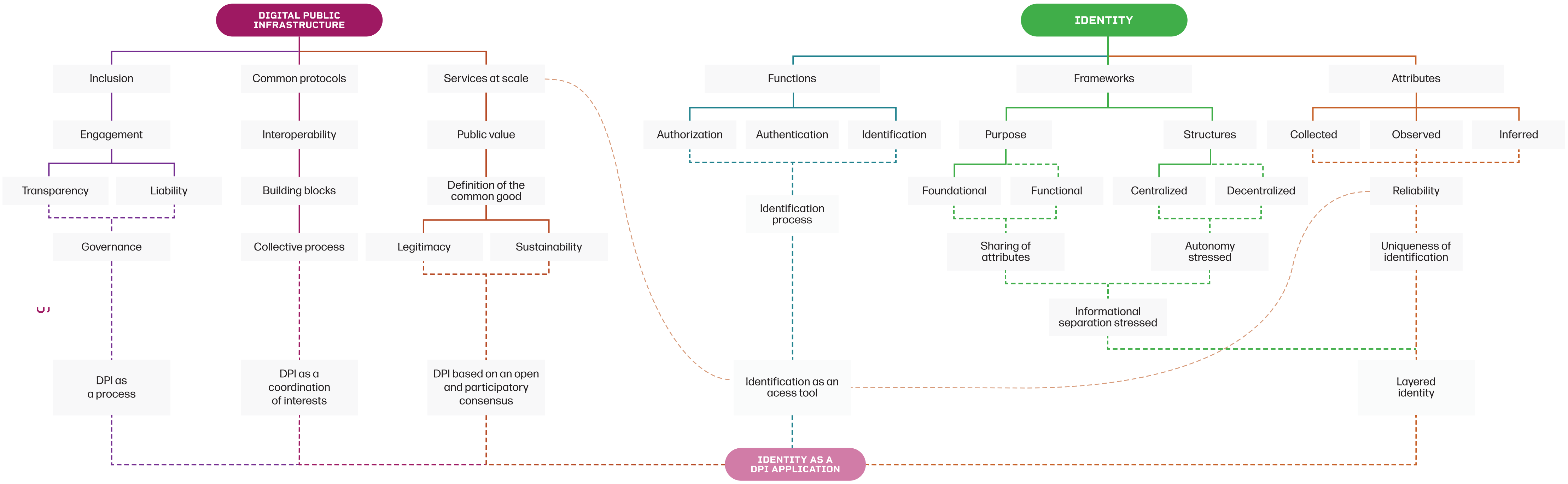
- Guarantee accountability tools for the agents involved in the development of the systems, so that they take responsibility for practices, especially those that impact vulnerable groups;
- Have participatory governance systems from the ground up, guaranteeing the effective participation of the various stakeholders, especially civil society and vulnerable groups who may be particularly affected by digital identity systems.

The integration of identity layers aims to increase trust in the systems, but the lack of governance may lead to rights violations. Therefore, its implementation requires careful approaches to ensure security, accountability and inclusion. 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.

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

The following mind map consolidates the assumptions, links and nuances of this DPI identity ecosystem:

MENTAL MAP


DIGITAL PUBLIC INFRASTRUCTURE
Inclusion
Common protocols
Services at scale
Engagement
Interoperability
Public value
Transparency
Liability
Building blocks
Definition of the common good
Governance
Collective process
Legitimacy
Sustainability
DPI as a process
DPI as a coordination of interests
DPI based on an open and participatory consensus
IDENTITY
Functions
Frameworks
Attributes
Authorization
Authentication
Identification
Purpose
Structures
Collected
Observed
Inferred
Identification process
Foundational
Functional
Centralized
Decentralized
Reliability
Sharing of attributes
Autonomy stressed
Uniqueness of identification
Informational separation stressed
Identification as an acess tool
Layered identity
IDENTITY AS A DPI APPLICATION

Summary

About the booklet

What is the purpose of this booklet?

This booklet has been designed as a resource for agents working in the identity ecosystem to recognize the foundations, applications and functionalities of a digital identity in the context of the DPI. The booklet organizes a diffuse mosaic of the role of identity in a DPI, based on examples, in order to shed light on the main key points for this infrastructure application to promote fundamental rights.

Who is the booklet's target audience?

Institutions, public bodies, companies and researchers who plan, develop and implement **digital identity functionalities or products**.

How to navigate the booklet?

EXEMPLE: CASE STUDY

! **Explanation box:** key concepts

1 IN PURSUIT OF CONSENSUS ON A DIGITAL PUBLIC INFRASTRUCTURE

Just as there is public investment in building physical infrastructure, such as roads, motorways and railways, there is an increasing need to implement a digital public infrastructure (DPI).

Even without realising it, people use physical infrastructure to access spaces in their daily lives. For people to visit public offices, banks, health clinics, shops and friends, they depend on infrastructure such as roads, avenues, buses, cars, petrol stations, bus stops, pedestrian crossings and pavements. However, people are increasingly using digital spaces to carry out these activities. It is possible and convenient to access bank accounts, talk to family and friends, pay taxes, make medical appointments and receive government benefits, among other things, without leaving home.

So, just as physical infrastructure is fundamental for carrying out everyday activities, the debate on building a digital infrastructure is gaining prominence. This structure is seen as a solution to simplify the flow of people and data, and thereby increase social wellbeing.

By aiming to rebuild and improve the foundational structures of the most diverse organisations, the development of a DPI can create exponential results for different sectors, such as finance, health, and commerce.

However, there is still no single concept of what a DPI is. Various organisations are debating the issue precisely in order to define the essential elements that make up a DPI application. Based on this definition, it would be possible to encourage and direct incentives towards homogeneous DPI applications that respect these parameters.

Given the potential of this infrastructure, the G20, especially during India's presidency, embraced the issue as a fundamental tool for providing public services at scale. From then on, directions for a DPI were outlined. The G20 itself[1] formulated a definition of what a DPI would be.

[1] G20. Compilation of documents annexed to the G20 New Delhi Leaders' Declaration and other official documents adopted during India's G20 Presidency. **G20 Digital Economy Ministers' Meeting Outcome Document and Chair's Summary**. Bengaluru, 19 Aug. 2023, p. 333. Available at: https://www.g20.in/content/dam/gtwenty/gtwenty_new/document/nov-23/Compilation_of_documents_annexed_to_the_G20_NDLD.pdf. Accessed on: 22 April 2024

As international debates on the concept and applications of a DPI progress, other players are joining in to shape what is understood as the application of this infrastructure. For example, for the World Bank[2], DPI would be like the "rails" that support transactions and inclusive digital connections between people, companies and governments, including the provision of services and operations in the public and private sectors.

The delimitation of these concepts helps to make sense of the direction of a DPI. Through the use of qualifiers such as "inclusive", "interoperable" and "involving different sectors", it is possible to outline the types and criteria for an application to be recognised globally as a DPI.

An inclusive DPI application means that it can be used by everyone who is interested, eliminating any discriminatory barriers.

DPI applications must be able to communicate with each other. Interoperable applications arise from the definition of standards that will allow data to be exchanged even between different systems.

As a rule, infrastructure solutions are planned and implemented by several players, since they impact not just one sector, but the whole of society. DPI applications must be the result of a joint effort by various social groups.

In 2024, the international debate takes on Brazilian frameworks. Brazil took over the presidency of the G20, bringing closer together discussions about the development and premises of a digital public infrastructure in Brazil. One of the factors that highlights this mix is the approval of a National Digital Government Strategy through Decree No. 12,069 of 21 June 2024[3].

The Decree aims to articulate the digital transformation strategies of the Brazilian public administration, at federal, state and municipal level. The Strategy is provided for in the Digital Government Law, Law 14.129, of 29 March 2021, and its text, which was in public consultation, is the result of a construction carried out by the Ministry of Management and Innovation in Public Services[4].

For the Decree, DPIs are solutions on a universal scale resulting from the orchestration of various players, whether from the public or private sector.

Each organization has presented different and specific descriptions and approaches to defining a DPI. Despite the diffusion of meanings, the definition of a DPI concept would make it possible to draw up global or even local guidelines for the development of this infrastructure.

[3] BRAZIL. Presidency of the Republic. **Decree no. 12.069, of 21 June 2024**. 2024. Available at: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2024/Decreto/D12069.htm. Accessed on: 24 June 2024.

[4] BRAZIL. Ministry of Management and Innovation. **Public Consultation - National Digital Government Strategy**. Brasília, 15 December 2023. Available at: https://dados.gov.br/dados/conteudo/consulta-publica-estrategia-nacional-de-governo-digital.

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.

With the assimilation of the G20 parameters by various organizations, it is possible to say that a level of consensus is forming regarding the characteristics of this system. The infrastructure must be made up of open, interoperable technology with transparent, accountable and participatory governance interfaces to enable innovation and the development of social value[5]. As an infrastructure, DPI applications are the result of a robust ecosystem of stakeholders, representatives of the public sector, the private sector or civil society. Thus, as well as driving innovation, these actors also guarantee the continuous development, trust and accountability of the infrastructure.

D + P + I

However, what does "**infrastructure**" mean in a DPI? Some categories of infrastructure are recognised as part of physical infrastructure, such as the transport network, energy generation and distribution, telecommunications structures, water distribution and sanitation. Even so, beyond these examples, it is still vague to define what infrastructure is. In everyday language, infrastructure can be understood as "things we use to build other things" or "the technology and systems needed for society to function"[6].

Despite the vagueness of what would be considered infrastructure, this is the key concept to avoid the concept of DPI being too broad[7]. In other words, because of the infrastructure in a DPI, it may not encompass different and divergent applications and thus makes the term meaningless. To define infrastructure, Professor Porteous uses the *Principles for Financial Market Infrastructures* (PFMI), published by the Bank for International Settlements. In this approach, two elements stand out:

- multilateral nature of infrastructure;
- the existence of an operator responsible for making the infrastructure work in an orchestrated way.

According to this proposed approach, solutions that do not allow interaction with various entities, people and organizations are services or applications that cannot be perceived as infrastructure. Furthermore, for the purposes of supervision and

[5] MASSALLY, Keyzom Ngodup, MATTHAN, Rahul, CHAUDHURI, Rudra. **What is the IPD Approach?** Carnegie Endowment for International Peace, 15 may 2023. Available at: https://carnegieindia.org/2023/05/15/what-is-dpi-approach-pub-89721. Accessed on: 27 January 2024.

[6] ZUCKERMAN, Ethan. **What Is Digital Public Infrastructure?** Center for Journalism and liberty, 17 nov. 2020. Available at: https://www.journalismliberty.org/publications/what-is-digital-public-infrastructure. Accessed on: 27 April 2024.

[7] PORTEOUS, David. **Is DPI a useful category or a shiny new distraction?** 2023. Available at: https://www.integralsolutionists.com/is-dpi-a-useful-category-or-a-shiny-new-distraction. Accessed on: 27 April 2024.

regulation, it is essential that there is an entity that operates the infrastructure. This element is stressed in the case of decentralized applications, such as the internet, where there is no single central authority responsible for the systems. However, despite the tension over this aspect, it is still useful for characterizing an infrastructure.

M-Pesa Case

Kenia has a mobile payment solution called M-Pesa. This solution is widely used and can be considered essential for small businesses. However, the solution is not truly multilateral, even though it involves other parties such as banks and service providers[8]. This is because the solution is centrally managed by the company Safaricom and it only allows the participation of a few entities, mainly banks, which have bilateral agreements with Safaricom[9], rather than being part of an open, interoperable system where multiple financial institutions can interact freely.

So, in general, infrastructure applications would be those used by the collective, with broad utility, beyond the needs of specific groups, and therefore accessed by the most diverse actors. Also, the infrastructure would be a set of systems that would allow people, governments and companies to relate to each other for purposes not limited by the infrastructure itself. In other words, it would act as an intermediary for applications developed on it, serving different needs and purposes.

D + P + I Another element of DPI is the sense of "**public**", since any digital infrastructure must be public to be considered a DPI. At first glance, it's important to note what a DPI is not.

Being a public infrastructure does not mean being the responsibility of a government, or even being owned or licensed by government entities. Furthermore, defining the parameters for an application to be considered public is an arduous and controversial task among people who research and implement these approaches.

[8] PORTEOUS, David. **Is DPI a useful category or a shiny new distraction?** 2023, p. 11. Available at: https://www.integralsolutionists.com/is-dpi-a-useful-category-or-a-shiny-new-distraction. Accessed on: 27 April 2024.

[9] DONOVAN, Kevin. Chapter 4. **Mobile Money for Financial Inclusion**. 2012. Available at: https://documents1.worldbank.org/curated/en/727791468337814878/585559324_201406191042051/additional/722360PUB0EPI00367926B9780821389911.pdf. Accessed on: 25 June 2024.

David Eaves and Mariana Mazzucato, Beatriz Vasconcellos, from the University of London (UCL)[10], understand that the meaning of a public infrastructure is reflected in maximizing the public value of that application. The first step would be to make the meaning of public value explicit. This concept is closely linked to what a society understands by the common good framework.

From Mazzucato's perspective, the common good[11] has five pillars:

- **Goal and direction:** Define an ambitious direction in which policies can be designed, public-private partnerships formed and citizens involved;
- **Co-creation and participation:** Defining the rules and mechanisms for co-investment, collaboration and coordination involving a diverse group of organizations;
- **Collective learning and knowledge sharing:** Rethinking institutional practices that support collective learning and develop long-term capacities and competences;
- **Access for all and benefit sharing:** Ensuring that public value is distributed equitably for and inclusive growth; and
- **Transparency and accountability:** Gaining and maintaining citizens' trust in monitoring progress through practices that demonstrate a commitment to transparency and accountability.

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[12]. 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 fulfill the specific aims and objectives of the community in which they are inserted.

In addition to the idea of the common good, aspects of governance and the role of

[10] EAVES, David; MAZZUCATO, Mariana; 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). Available at: https://www.ucl.ac.uk/bartlett/public-purpose/sites/bartlett_public_purpose/files/iipp_wp_2024-05.pdf. Accessed on: 25 April 2024.

[11] 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.

[12] 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.

the state must be taken into account when identifying a DPI. This is because the process of understanding what is considered public value is just as important as the outcome itself and must be conducted in a collective and coordinated manner. It is therefore essential to create governance structures so that the different stakeholders can move forward collectively towards the common good[13].

Understanding what is considered to be public value through a process is essential to ensuring that DPI initiatives truly meet the needs and aspirations of the community. This understanding not only directs efforts effectively, but also guarantees the legitimacy and sustainability of the results achieved. With this, the coordination of interests in the process is essential to ensure that diverse perspectives and interests are considered, promoting an open and participatory consensus on what constitutes public value. Therefore, investing in governance structures that promote active participation and coordination between all stakeholders is key to maximizing public value.

Payment system developed by a payment card company:

It can be argued that the evolution of payment methods has contributed to financial inclusion and people's participation in the global digital economy. However, according to Eaves, Mazzucato and Vasconcellos, the creation of public value means that widely accepted social objectives can be achieved in processes of collaborative innovation between different actors who co-create markets. To effectively generate such results, it is essential to make expertise available in planning, implementation, management and coordination between various interest groups. This was not necessarily the process embraced by the payment system in question, which is why the interpretation that these systems constitute DPI is questionable.

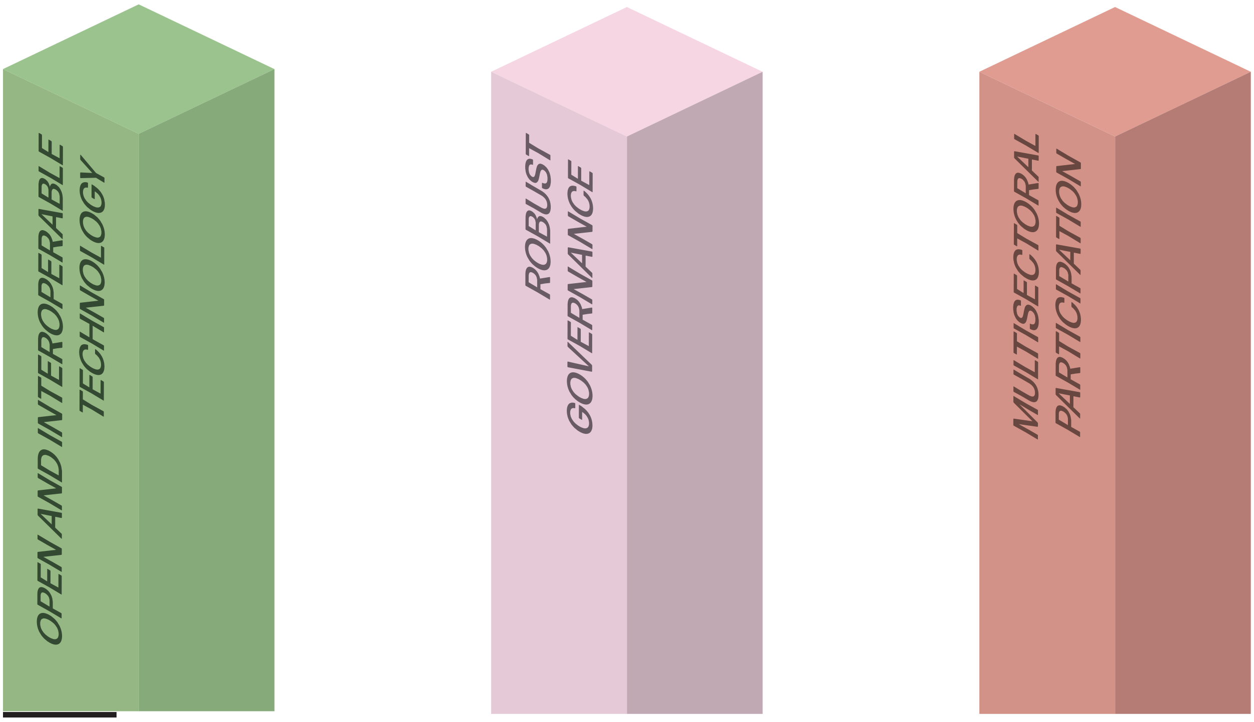
D + P + I The term "**digital**" in DPI does not restrict the concept of digital public infrastructure, depending on the level of intensity of its digitisation. There seems to be little benefit in restricting DPI to a few types of digital applications, but it is relevant to note the existing gradations of digitalisation[14]. As an example, the OECD has proposed a classification of digitalisation into three levels: a core layer, where only electronic devices such as computers and mobile phones

[14] PORTEOUS, David. **Is DPI a useful category or a shiny new distraction?** 2023, p. 11. Available at: https://www.integralsolutionists.com/is-dpi-a-useful-category-or-a-shiny-new-distraction. Accessed on: 27 April 2024.

are used; a narrow layer, which includes carrying out activities digitally; and a broad layer, where activities have been significantly enhanced by digital technologies and data[15]. Even with this gradation, different types of applications can be considered digital.

Given the difficulty of defining objective parameters for what DPI applications are, some definitions limit themselves to listing the three sectors that are recognised as DPI. These sectors are payments, identity and data sharing. This way of defining DPI does not restrict the concept to just these sectors, but creates the inference that, for other sectors to be added, they would have to demonstrate strong similarities with these three main sectors[16].

n the other hand, some seek to understand DPI based on its fundamental elements. In the sense presented by the G20, DPI is based on **three pillars**: (i) open and interoperable technology, (ii) robust governance, and (iii) multisectoral participation[17]. Without these elements, the DPI's objectives are likely to be greatly hampered and limited to a specific group, without producing the general impact that is intended.


OPEN AND INTEROPERABLE TECHNOLOGY
ROBUST GOVERNANCE
MULTISECTORAL PARTICIPATION

[15] OECD. **Handbook on Measuring Digital Platform Employment and Work**. 3. Conceptual framework, concepts and definitions. 2023. Available at: https://www.oecd-ilibrary.org/sites/2d333ec3-en/index.html?itemId=/content/component/2d333ec3-en. Accessed on: 25 April 2024.

[16] PORTEOUS, David. **Is DPI a useful category or a shiny new distraction?** 2023, p. 11. Available at: https://www.integralsolutionists.com/is-dpi-a-useful-category-or-a-shiny-new-distraction. Accessed on: 27 April 2024.

[17] UNDP. **The DPI Approach: A Playbook**. 21 Aug. 2023. Available at: https://www.undp.org/publications/dpi-approach-playbook. Accessed on: 27 March 2024.

OPEN AND INTEROPERABLE TECHNOLOGY

The first concept indicates that the infrastructure should be designed using **common protocols** so that other functionalities can be added to it and these can interact with each other. The ecosystem should be built on the principles of openness, interoperability and scalability, so that independent modules can be added and improved as the infrastructure develops. It is essential that communication and the exchange of information between systems is possible in order to generate trust and facilitate the flow of data.

In the context of DPI, the concepts of interoperability and scalability are fundamental to ensuring that the system is efficient, flexible and capable of evolving as demand grows. Scalability is precisely the ability of a system to efficiently increase its capacity and functionality as demand grows, without compromising the performance or quality of the services offered. As will be seen in this section, interoperability refers to the ability of different systems, devices, applications or services to communicate, exchange data and use this information in a coordinated and efficient manner, regardless of their origins or platforms.

From the exchange of information between systems, other characteristics of the technology emerge as the basis for DPI, such as extensibility and scalability[18]. These elements point to a "building blocks" approach, in which it is possible to accommodate changes and increase the functionality of the infrastructure without losing its previous functionality, allowing for updates and improvements whenever necessary. With this, the technology used to build a DPI allows independent modules to be added and improved as the infrastructure develops.

The second element determines that the DPI ecosystem complies with **governance** parameters, i.e. the infrastructure must be reliable, transparent and accountable. One of the uses of governance is to allow legal obligations to be incorporated directly into the infrastructure architecture, ensuring that agents comply with the law through the simple act of participation. By default, sectoral regulations would be complied with, since the system would be compliant, including with personal data protection standards, which is one of the rights most under strain in the context of a DPI.

ROBUST GOVERNANCE

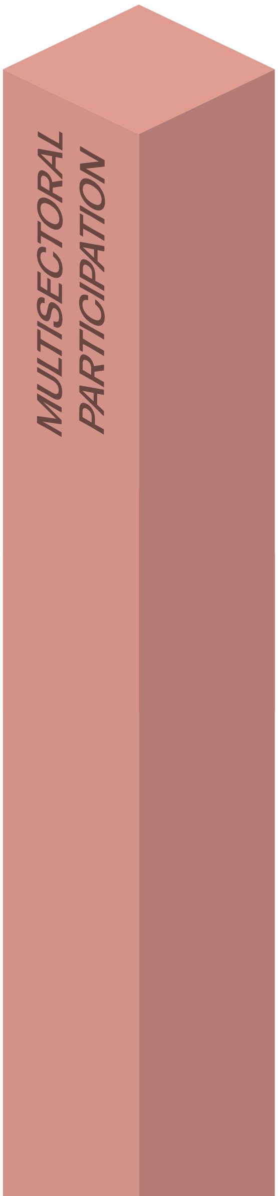
[18] UNDP. **The DPI Approach: A Playbook**. 21 Aug. 2023. Available at: https://www.undp.org/publications/dpi-approach-playbook. Accessed on: 27 March 2024.

A system with robust governance means that it is designed in such a way that legal compliance is integrated and automatic. This is a challenge for DPI application developers, but in order to be considered DPI, the application must be designed so that legal compliance is integrated and automatic.

In practice, this translates into designing systems with built-in rules, such as data protection mechanisms that guarantee users' privacy in accordance with regulations. This can include encryption, access control and data anonymisation. In addition, cybersecurity and authentication protocols must be integrated to protect against unauthorized access and guarantee data integrity. These tools reinforce the understanding that the development of DPI applications is a process of constant evaluation and improvement, only in this way can they realize the pillars of a DPI.

Implementing governance parameters implies maximizing the benefit to citizens, trust and transparency that ensure that DPI is safe, secure, reliable and accountable[19]. Governance also promotes inclusion, since while conducting the processes necessary for DPI governance, inclusion parameters must invariably be addressed[20].

The element of **active participation** by different sectors of society in building the DPI highlights the importance of innovation in the market and the provision of services to enhance people's experiences. 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 user of that application. Co-operation between actors enables the development of innovative solutions and the sustainability of the system[21]. By allowing other groups to actively contribute, governments can create a more dynamic, sustainable and inclusive digital ecosystem.



[19] UNDP. **The DPI Approach: A Playbook**. 21 Aug. 2023. Available at: https://www.undp.org/publications/dpi-approach-playbook. Accessed on: 27 March 2024.

[20] EAVES, David; MAZZUCATO, Mariana; 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). Available at: https://www.ucl.ac.uk/bartlett/public-purpose/sites/bartlett_public_purpose/files/iipp_wp_2024-05.pdf. Accessed on: 25 April 2024.

[21] MASSALLY, Keyzom Ngodup, MATTHAN, Rahul, CHAUDHURI, Rudra. **What is the DPI Approach?** Carnegie Endowment for International Peace, 15 May 2023. Available at: https://carnegieindia.org/2023/05/15/what-is-dpi-approach-pub-89721. Accessed on: 27 January 2024.

For an application to be considered part of a DPI, it is essential that there is a formal aspect of participation that goes beyond mere consultative guidance and establishes itself as a fundamental and binding element. The effective participation of society with the power to decide and direct the guidelines is a prerequisite without which there can be no development of DPI. Therefore, the proceduralisation of this participation must cover the entire chain of development and implementation of the application, defining minimum rules and mechanisms that guarantee the effective inclusion of vulnerable groups.

This could include, for example, earmarking part of the DPI's resources to fund research into the impact of implementation, as well as offers of aid for civil society representatives to actively participate in multisectoral discussion forums. Furthermore, this participation must be binding, allowing public scrutiny to have the power to block proposals or change their direction, ensuring a truly deliberative process and not just a consultative one.

The participation pillar, together with robust governance, ensures that the infrastructure's objectives are achieved in a broad and inclusive manner. In this sense, a robust system must provide society with spaces to improve applications by identifying challenges and points for improvement based on the experience of citizens, since they are in contact with the application's functionalities and those responsible for its development.

In this sense, although a DPI is complex and made up of various elements and actors, it is through the implementation of a digital ecosystem that countries seek to boost inclusive growth, innovation and training. Digital infrastructure is a tool that has already been implemented at some level by many countries. In these cases, it is perceived as a bridge to facilitate the inclusion, efficiency and empowerment of the population in the face of the common activities of a society[22].

Brazil is one of the countries that is moving towards consolidating a digital public infrastructure across various sectors, in order to impact not only how public services are provided, but also any other activity or service used by citizens. Brazil is already leading global discussions on technological infrastructure in the financial sector, with the development of Pix, and in access to public services, with Gov.br.

[22] MASSALLY, Keyzom Ngodup, MATTHAN, Rahul, CHAUDHURI, Rudra. **What is the DPI Approach?** Carnegie Endowment for International Peace, 15 May 2023. Available at: https://carnegieindia.org/2023/05/15/what-is-dpi-approach-pub-89721. Accessed on: 27 January 2024.

Building a solid and effective DPI depends intrinsically on its pillars of open and interoperable technology, robust governance and multisectoral engagement. The adoption of open and interoperable technologies ensures that systems are flexible, accessible and able to communicate with each other, promoting innovation and the improvement of systems. Robust governance ensures that decisions are made in a transparent and accountable manner, while active social participation, especially with mechanisms that allow for the inclusion of vulnerable groups, ensures that the diverse voices of society are heard and considered. Together, these foundations not only enhance the impact of DPI, but also promote equitable and sustainable development.

2 DIGITAL IDENTITY: ONE OF THE KEY APPLICATIONS OF DPI AND ITS TYPICAL FUNCTIONS

One of the fundamental points of the transformation driven by a 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 the operation of digital systems and services, while these systems can only function if it is possible to identify the beneficiary of the applications in a secure and convenient way. As part of the relationship becomes 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 whether the person behind the screen is really who they say they are.

It is through identity validations, whether online or offline, that people access essential services, whether public or private, national or international. In some applications, identity is the gateway to the digital world, which increases the demand for a robust and reliable validation process.

For example, in order for a bank to grant a loan to a customer, it must know who it is contracting with and what the characteristics of that person are. The same situation is replicated for accessing a social benefit and for a medical consultation, among others. This identity information can be dispersed in different and complementary frames or layers, collected in different contexts, as will be described in the next section of this booklet.

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 by means of a document issued by the state. In the case of a bank transfer, it is expected that certain security and integrity requirements will be guaranteed in order to confirm the identity of those involved in the process.

How can this process be made digital without it ceasing to be reliable? A digital identity is seen as another way of facilitating the process of identity authentication, making access to goods and services safer and less bureaucratic.

According to the OECD, a **digital identity** is a set of attributes collected and stored electronically that can be used to prove a characteristic, quality or assertion about a citizen and, when necessary, support the unique identification of that user[23]. With this tool, it is possible to simplify access to various services by adding an optional alternative to verifying physical credentials and thus strengthen a DPI approach.

Credentials: An object or data structure that authoritatively links an identity (and optionally, additional attributes) to a token owned and controlled by an entity trusted by the credential provider[24].

Personal Identifiable Information (PII): information used to uniquely identify, contact or locate a person.

In this infrastructure, new tools are being developed to conduct reliable and protective identification processes, since they create value for organizations and governments based on the identity of users. It should be noted that one of the characteristics of identification, in terms of the OECD concept, is its uniqueness, i.e. it is only possible to identify an entity if only it has that identity.

This **uniqueness** of identity creates a tension that is even more aggravated in the digital context. It is common for a person to have different attributes and to use some of them whenever necessary. Depending on the context, a person can identify as a teacher, a sister, a daughter, a hospital patient, a shop customer or a member of a sports academy, without having to be all of these attributes at once[25]. This fragmentation of identity is quite common, but controversial in digital contexts, where it is possible to group together and make available a series of attributes of a person, even if they are only useful in different contexts.

Identity solutions are complex precisely because of the multidisciplinary nature they affect, from legal effects to public policies, consumption, personality and cultural impacts. Given the diversity of areas affected, technologies that make use of big

[23] OECD. OECD/LEGAL/0491. **Recommendation of the Council on the Governance of Digital Identity**. 8 Jun. 2023. Available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0491. Accessed on: 27 January 2024.

[24] NIST. **Withdrawn NIST Technical Series Publication**. 3 Jul. 2019, p. 51. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf. Accessed on: 2 May 2024.

[25] CARIBOU DIGITAL. **Identities: New practices in a connected age**. Farnham, Surrey, United Kingdom: Caribou Digital Publishing, 2017. Available at: https://www.identitiesproject.com/wp-content/uploads/2017/11/Identities-Report.pdf. Accessed on: 2 June 2024.

data, the guarantee of interoperability of this system, the centralisation or decentralisation of databases, blockchain registries, and the collection of biometrics as information to prove uniqueness, bring a new layer of complexity to this scenario. The establishment of unique identifiers or the dispersion of these attributes point to new challenges in this area.

While identity verification is a useful process, there is still little clarity about what requirements a digital identity solution must have in order to be recognised as sufficient to identify and be digital. This is because there is no definition of which functionalities are necessary for the system to be considered an identity system and thus to be a digital identity system. The common elements of these systems, and therefore their possible frameworks, will be analysed in the next chapter.

The World Bank understands digital identification systems to be those that use technology throughout the identity lifecycle, including for data capture, validation, storage and transfer, credential management, verification and authentication[26]. This definition recognises that identity can be provided directly by the government, in partnership or outsourced to the private sector. However, despite having this flexibility in issuance, as a rule, digital identity is linked to a person's legal identity, which is recognised by the government for use for official purposes.

It is important to note that a digital identity, even if it is part of a DPI context, is not to be confused with a **legal identity**, which is the recognition of a person as a subject of rights and duties by a state[27]. Legal identity is a human right, according to Article 6 of the Universal Declaration of Human Rights[28], and access to a legal identity is objective 16.9 of the Sustainable Development Goals (SDGs) defined by the United Nations (UN)[29]. At the same time, identity systems, whether online or offline, have similarities, such as their function.

Despite the difference in concepts, there is an intersection between the themes. There is currently a significant identity gap in the world: it is estimated that approximately

[26] WORLD BANK. **Technology Landscape for Digital Identification**. Washington: World Bank License, 2018. Available at: https://documents1.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf. Accessed on: 27 January 2024.

[27] FUNDACIÓN KARISMA. **Conceptos básicos de los sistemas de identidad**. 7 Dec. 2021. Available at: https://digitalid.karisma.org.co/2021/12/07/conceptos-basicos-id/. Accessed on: 27 January 2024.

[28] UN. **Universal Declaration of Human Rights**. Adopted and proclaimed by the United Nations General Assembly (resolution 217 A III) on 10 December 1948. Available at: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Accessed on: 28 January 2024.

[29] UN. **Sustainable Development Goal 16: Peace, Justice and Strong Institutions**. Available at: https://brasil.un.org/pt-br/sdgs/16. Accessed on: 28 January 2024.

1 billion people do not have an official identity document. The lack of an identity document excludes these people from access to essential services, whether public or private. The UN has realised that by disseminating digital solutions it would be possible to ensure that more people have a legal identity[30].

CIN (Brasil)

The new Brazilian legal identity is issued on paper and digitally. The CIN is on the Gov.br app. With a legal identity, on paper, the person also has access to other digital public services provided by Gov.br access.

Although it varies according to its elements and moldings, any identity system has three basic **functions**[31]:

- Identify,
- Authenticate, and
- Authorize.

The **identification** function determines the registration of a person by collecting personal biographical information and issuing credentials so that an identity can be proved. This information is usually collected by presenting civil registration documents, such as a birth certificate or marriage certificate..

!

Biographical data: minimum personal data recorded about a person. This data may vary depending on the authority issuing the credential. In the European Union, the minimum data is: (1) current family name(s), (2) current name(s), (3) date of birth and (4) a unique identifier. Additional attributes include: (5) surname at birth, (6) first name at birth, (7) place of birth, (8) current address and (9) gender[32].

[30] UNDP. **How digital can close the 'identity gap'**. 19 May 2022. Available at: https://www.undp.org/blog/how-digital-can-close-identity-gap.

[31] WORLD BANK. **ID4D Practitioner's Guide: Version 1.0**. Washington: World Bank License, out. 2019. Available at: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf. Accessed on: 28 January 2024.

[32] WORLD BANK. **ID4D Practitioner's Guide: Version 1.0**. Washington: World Bank License, out. 2019. Available at: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf. Accessed on: 28 January 2024.

As a rule, this function of the identity system is achieved through actions carried out by the public authorities in the place where the civil registration documents were issued. Once the information has been collected, it can be verified, at which point a link is established between a claimed identity and the person presenting the evidence. However, some people do not have any registration documents. In these situations, identification systems can verify the person's identity and address in another way[33].

Once the verification has been completed, it is possible that some duplicity will be identified in the issuing of the document, some biometric records will be collected and the identification document will be issued. This document is the credential that will be used in subsequent interactions. This credential can be physical or digital, but it is essential that it is interoperable for authentication, so that other people can check its validity.

eID (European Union)[34]

Electronic identification (eID), the result of the eIDAS Regulation (910/2014), is a set of services provided by the European Commission to enable the mutual recognition of national eID systems across borders in each EU country. eID allows European citizens to use their national eIDs when accessing online services from other European countries. The system guarantees legal, organizational, semantic and technical interoperability in order to validate identities issued by other entities and thereby facilitate digital operations that require cross-border identity recognition.

Authentication is the possibility 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 responsible for a given identity claims to have, know or be. As a rule, these factors are the passwords a person knows, the biometric information they present, access to a service they already have, a token, or a combination of these elements.

[33] WORLD BANK. **Technology Landscape for Digital Identification**. Washington: World Bank License, 2018, p. 5. Available at: https://documents1.worldbank.org/curated/en/199411519691370495/Technology-Landscape-for-Digital-Identification.pdf. Accessed on: 5 May 2024.

[34] EUROPEAN UNION. European Commission. **How does it work?** 2024. Available at: https://ec.europa.eu/digital-building-blocks/sites/pages/viewpage.action?pageId=467109866. Accessed on: 2 May 2024.

Something a person...

HAS	KNOWS	IS
card	password	fingerprint
certificate	passphrase	irises
security token	PIN	face
mobile app	challenge-response	behavior
access badge	other secret	biographic data

Inspired by *ID4D Practitioner's Guide*[35]

Authentication systems tend to be more secure if they combine more than one of these factors, so that, for example, the person demonstrates that they know the password for an application and have a trusted device, such as a mobile phone or a password. This combination of factors is known as double authentication.

At this point, some challenges are already known: reducing processing time, improving authentication accuracy, guaranteeing a low-barrier experience for people, mitigating challenges with network connectivity, combating fraudulent behavior and finding affordable hardware and software solutions. So it's not enough for a person to identify themselves, to say who they are, they must be able to prove that they are who they say they are. Their identity must be identifiable.

Background check in a job interview

When a person applies for a job, recruiters may ask for documents that prove their previous experience, as well as their academic credentials. These recruiters may check the validity of a bachelor's degree based on the information provided on the degree itself, as well as on the document authentication system of the university that issued the credential.

The **authorisation** function determines whether a person with an authenticated identity can access specific services or information, appropriate and limited to their level of access. Once an identity has been authenticated, the access rights that an

[35] WORLD BANK. **ID4D Practitioner's Guide: Version 1.0**. Washington: World Bank License, out. 2019, p. 20. Available at: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf. Accessed on: 28 January 2024.

organization has associated with that identity are defined. In more complex authorisation systems, access rules can be contextual and dynamic.

Traffic stop

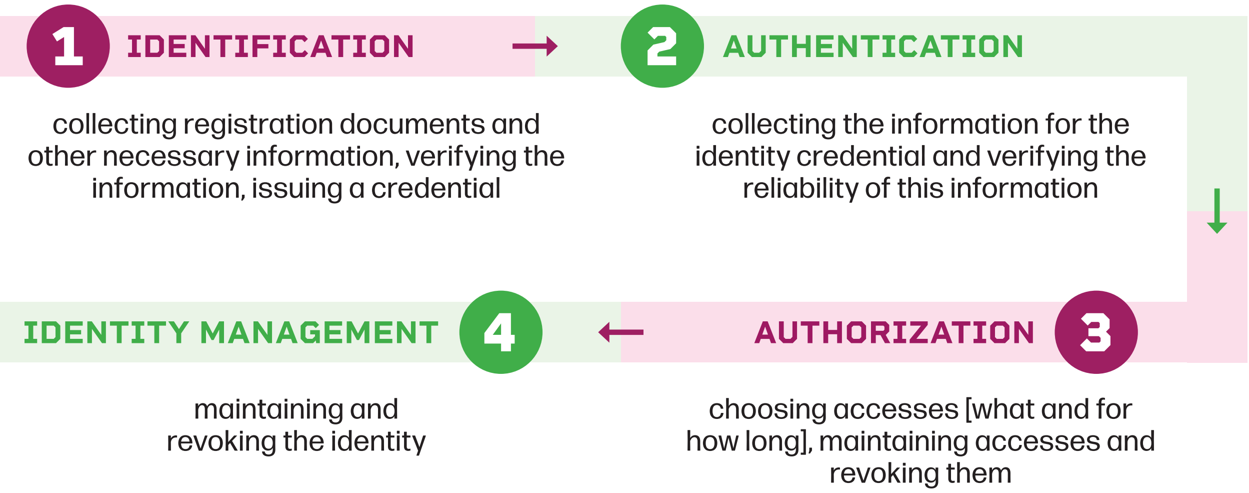
It is common for police forces to carry out identity checks on people driving vehicles. In these processes, the authorities check the authenticity of the identity, as well as the authorisations guaranteed by the identity card credential. This is the case of an authority checking a person driving a lorry. If the person driving the vehicle, despite having an authentic driving license, is not authorized to drive a lorry, their identity limits the access they have.

Identity systems are fundamental to the provision of services and the fulfillment of rights and obligations. These systems must fulfill the identity functions that are common to any identity system, regardless of whether the system is part of a DPI or not.

In some situations, both public and private sector institutions need to know who the people they are dealing with are. Also, for basic economic, social, political and digital transactions, these entities must be able to trust that people are who they say they are, i.e. that no one has stolen or hacked their identity credentials. In addition, these entities may need to confirm, either during the initial onboarding of a new beneficiary or customer, or on an ongoing basis, that the person is eligible to access a particular right, service, information or system functionality[36]. In this way, it is clear that the functions of identity systems are exercised at different times to guarantee confidence in the application used.

These functions are not independent of each other, but are intertwined and converge in the specific context of application. According to the World Bank, they form a cycle in which, from identification, it is possible to authenticate and authorize access until the identity is revoked. This happens, for example, when the identified person dies.

[36] WORLD BANK. **ID4D Practitioner's Guide: Version 1.0**. Washington: World Bank License, out. 2019, p. 20. Available at: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf. Accessed on: 28 January 2024.



1 IDENTIFICATION

collecting registration documents and other necessary information, verifying the information, issuing a credential

2 AUTHENTICATION

collecting the information for the identity credential and verifying the reliability of this information

3 AUTHORIZATION

choosing accesses [what and for how long], maintaining accesses and revoking them

4 IDENTITY MANAGEMENT

maintaining and revoking the identity

The development of digital identity systems, as one of the key applications of DPI, is being endorsed by international organizations, especially in view of SDG target 16.9[37]. At the same time, in order for it to be recognised as part of DPI, it is essential to be able to highlight how ID applications make up a digital infrastructure in order to generate public value according to the functions these systems have. Through digital identity verification processes, it is possible to guarantee access to benefits, rights and services for those people who are entitled to them.

In the digital world, given the demands, above all, of preventing fraud and guaranteeing trust in digital relationships, the elements that make up an identity system have become complex. In addition to the fact that there is no definition of the requirements for a digital identity, identification systems can be made up of various elements and assumptions that form their own molds.

In turn, these molds delimit the structure that these systems can have, including their functionalities. It is therefore necessary to consolidate consensus and make progress on the issue so that it is possible to develop a citizen digital identity, i.e. one with a strong foundation in the values of a DPI.

[37] EAVES, David; MAZZUCATO, Mariana; 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). p. 17. Available at: https://www.ucl.ac.uk/bartlett/public-purpose/sites/bartlett_public_purpose/files/iipp_wp_2024-05.pdf. Accessed on: 25 April 2024.

3 POSSIBLE FRAMEWORKS FOR IDENTITY SYSTEMS

With technological advances, various identity systems have been developed by different organizations, both public and private, for different purposes. All these applications have in common the aim of creating and confirming credentials at specific times and in specific contexts, guaranteeing that the person has something in common or is the same as the person who first registered. It is because of this element that various solutions can be perceived as identity systems. Based on the similarities between these systems, four possible molds that reflect the peculiar elements of this identity ecosystem will be presented.

It's worth noting that these molds don't take into account the requirements of a digital public infrastructure, as they reflect the demands of identification systems without claiming to be validated by the parameters of a DPI - a cross-reference that will be made in the next section. Even so, these molds are important in the construction of a digital identity as an application of DPI, in order to understand the concrete variations of these systems.

3.1 Entities involved in the system

An identity system can be organized in a simple or complex way, depending on the number of entities involved in its implementation.

As a rule, a more traditional system, especially one linked to the identification function, involves few entities in its implementation. This is why they are perceived as **simple**.

The simple system is made up of two actors: an identifiable person and an entity responsible for identification. This entity, which takes on various roles to enable identification, issues an identity and, on the basis of the credentials issued by itself, recognises the identified person. In simple systems, it is possible for the person and the entity to recognise each other or for them to divide their roles between user and identity service provider.

Thus, with fewer players involved, the trust model in the simple system identity is less complex, since there are fewer potential points of failure or breach of trust. At the same time, this simplicity can hinder the scalability and interoperability of the system.

In this system, only the entity that identifies can validate that identity, which can make the system unsuitable for the interaction of several users who frequently need to confirm their identity. Furthermore, in a simple system, the identity verification process does not depend on the collaboration of other entities and may not be compatible with other systems - both in terms of technological arrangement and the requirements for recognising this verification. This lack of interoperability can make integration with external services, organizations or ecosystems difficult or impossible.

Complex identity systems, on the other hand, are made up of various actors who coexist to fulfil different and complementary functions to make up the identity ecosystem. These systems can be made up of several actors who, as a rule, have the following functions[38]:

- **Person:** someone who needs to be identified, who needs an identity to access spaces and systems;

! In addition to systems for identifying people, there are systems for identifying electronic devices, objects and other living beings, which will not be explored in this booklet, although they are useful in certain contexts and have their own complexities.

- **Legal representative:** to whom the person, the subject of the identity, gives powers to act on their behalf, such as the guardians of a child, who act on their behalf;
- **Identity provider:** the entity responsible for issuing the identity and controlling the identity data, which is usually collected and stored by the provider;
- **Identity system operator:** entity contracted by the identity provider to carry out certain functions delegated by it, such as providing technological services for the system's operation;

[38] WORLD ECONOMIC FORUM. **Identity in a Digital World: A new chapter in the social contract**. Geneve: Sep. 2018, p. 14. Available at: https://www3.weforum.org/docs/WEF_INSIGHT_REPORT_Digital%20Identity.pdf. Accessed on: 25 May 2024.

- **Devices, groups of devices, physical and virtual assets:** the means that people have or use to access their identity and which may have their own identifiers, such as the IMEI of a mobile phone;
- **Trusted entities:** entities authorized by the provider to confirm dispatch;
- **Trusted parties:** organizations that rely on the identities issued by the provider or those confirmed by the trusted entities to allow or deny access to goods, services, rights or information;
- **Regulators:** those who guide the way identities are managed and used.

It is important to note that the function of verifying and authenticating identity can be a shared service provided by the provider to public and private sector entities. This occurs in cases where the identity system allows users to take advantage of the credentials and authentication carried out by the system itself, making it unnecessary to build parallel authentication systems independent of the provider[39]. Thus, the entity that must conduct the identification process does not necessarily need to create its own system for authenticating this identity or issuing a new identity, it can use a system that has already been created, becoming a trusted part of the system.

Another possibility is that these entities that conduct identification processes do so as a trusted party of trusted entities. This means that the organization that identifies does not necessarily know the credentials and data of the people identified, but trusts the authentication made by the trusted entity.

Compared to a simple system, several agents can assign and validate identities, and it is also possible for other agents to make up the ecosystem to support its development on other fronts. In view of the multiplicity of actors, these systems are also characterized by the multiplicity of those responsible, since each one performs specific functions.

Complex systems are the result of demands for identification in both the analogue and digital worlds. In a Big Data scenario, identity systems are now made up of various entities, whether for accessing public policies, registering for e-commerce or streaming, complying with tax obligations, making a bank transfer, serving a subpoena in a court case, or pricing an insurance service, for example.

[39] WORLD BANK. ID4D **Practitioner's Guide: Version 1.0.** Washington: World Bank License, out. 2019, p. 15. Available at: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf. Accessed on: 28 January 2024.

It is common for people to identify themselves in different ways and for different purposes, in specific contexts. In addition, people may not be identified based on what they are, know or have, but rather on personal information shared by other organizations. In this scenario, the notion of identity has a direct impact on the activities of sharing personal data between entities, inferring information, integrating systems and cross-referencing data, including personal data. All these elements are amplified in a complex identity system made up of various actors.

System agents

Maria is a professional who recently applied for a loan to buy a car. To do this, she provided the bank with her personal information, such as her name, social security number, address, employment history and other relevant data. The bank, in turn, uses this data to assess Maria's credibility.

Participating organizations:

Bank: The bank sends Maria's details to a credit bureau to obtain a credit report. The report includes information about Maria's payment history, any outstanding debts, and other factors that influence her credit score.

Credit bureau: The credit bureau aggregates the data received from the bank with other information already in its system, collected from various sources such as retail shops, credit card operators and utilities.

Other entities: In addition to the sources mentioned, the credit bureau can receive information from other entities, such as courts (about legal proceedings involving Maria), social networks (which can provide inferences about Maria's behavior and financial stability) and financial institutions with which Maria has already had dealings.

Based on the data received from various sources, the credit bureau can infer additional information about Maria. These inferences are not only based on the information she has provided directly to the bank, but also on aggregated data from various other sources, many of which she may not even be aware of. In a complex system, Maria may not only be identified by what she is, knows or possesses, but also by information inferred and shared by other entities.

Identity solutions are thus becoming increasingly interwoven, including the addition of new functionalities based on the role of each agent. These systems come to be understood in terms of moldings and layers, implying new challenges, including in relation to the specific aims and purposes of the identity system constructed.

3.2 System structure

The structure of an identity system refers to the way the system's components and actors are managed and interact. This structure can vary depending on the context and the demands that the identity system aims to meet, including the way in which the data and entities involved are recorded and organized, and the level of control over identity.

In a **centralized** structure, there is only one provider for an identification system[40]. Essa entidade é responsável por toda a cadeia do sistema, inclusive pelas funções de checagem de identidade, emissão de credenciais, autenticação e armazenamento de dados.

In this case, the provider itself is the only agent offering services based on the identity it issues. Each service provider supplies the identifier (e.g. username) and the corresponding credential (e.g. password) to customers who wish to receive their services[41]. This structure is commonly used in login services in general, such as a social network, an e-commerce site or a bank, where in each service the person has their own credentials.

! One of the advances in identification systems is the implementation of a single sign-on (SSO) service. Through this service, the identity provider allows identified people to interact with other organizations without having to carry out a manual authentication process with each of them. They can use the credentials issued by one entity and recognised by all the others, which perceive them as a valid form of authentication[42].

[40] WANGHAM, Michelle *et al*. Chapter 1. **Federated Identity Management**. 2010, p. 8. Available at: https://www.researchgate.net/publication/228401861_Gerenciamento_de_Identidades_Federadas. Accessed on: 28 June 2024.

[41] FERDOUS, Md Sadek; CHOWDHURY, Farida; ALASSAFI, Madini. **In Search of Self-Sovereign Identity Leveraging Blockchain Technology**. IEEE Access, v. 7, 2019. Available at: https://ieeexplore.ieee.org/document/8776589. Accessed on: 28 June 2024.

[42] WANGHAM, Michelle *et al*. Chapter 1. **Federated Identity Management**. 2010, p. 8. Available at: https://www.

The characteristic element of a centralized structure is that the central authority has total control over the system. It can even share identity information and validate it with third parties, without the identified persons being aware of this sharing[43]. This authority, as the entity that knows and issues the identity, would have sufficient tools to use this data autonomously.

Currently, most identities and related data are managed by identity providers and are not controlled by the person themselves. As well as being vulnerable to hackers and improper sharing of information, this centralized model prevents users from having full control over their personal data[44]. It was in this context that other structures were devised.

A **federated** structure involves a single identity provider and one or more service providers, the relying parties. The identity provider issues identifiers and the corresponding credentials to the person and the service providers rely on the identity provider to authenticate the user and provide the user's attributes and their values to the service providers[45].

To access any service, people authenticate themselves at the identity provider and, once authenticated, are redirected to the service provider to access the service. Once a user is authenticated at the identity provider, they can access services from all the service providers that share the same identity provider. The shared identity domain is known as a federated identity domain and is created when a notion of trust is established between the identity provider and the corresponding service providers.

As a rule, this notion of trust is the result of establishing a contract between the corresponding entities. Decentralization is also the result of robust identity systems, with new actors and functionalities that interact with each other.

researchgate.net/publication/228401861_Gerenciamento_de_Identidades_Federadas. Accessed on: 28 June 2024.

[43] BIONI, Bruno; GARROTE, Marina; MEIRA, Marina; PASCHOALINI, Nathan. **Between visibility and exclusion: mapping the risks of National Civil Identification and the use of its database for the gov.br platform**. Data Privacy Brasil Research Association, 2022, p. 38.

[44] LEITE, Raquel Pereira; HENRIQUES, Marco Aurélio Amaral. **Feasibility analysis for implementing an authentication system based on Federated Digital Identities and Decentralised Digital Identities**. Campinas, p. 2. Available at: https://sol.sbc.org.br/index.php/sbseg_estendido/article/view/21714/21538. Accessed on: 28 June 2024.

[45] FERDOUS, Md Sadek; CHOWDHURY, Farida; ALASSAFI, Madini. **In Search of Self-Sovereign Identity Leveraging Blockchain Technology**. IEEE Access, v. 7, 2019. Available at: https://ieeexplore.ieee.org/document/8776589. Accessed on: 28 June 2024.

A shopping experience based on federated identity

Lucas decided to buy a new laptop. He opened his browser and accessed his favorite online shopping platform, where the shopping experience is facilitated by the federated identity model. On this platform, the Shopping Platform Account System acts as the Identity Provider, while the Product Catalog Service, Order Management Service and Customer Support Service are the Service Providers.

- **Logging in:** Lucas clicked on the login button on the home page. He was redirected to the login page of the Procurement Platform Account System, the Identity Provider. Lucas entered his e-mail address and password. The platform verified his credentials and authenticated him, issuing a token. This token would allow Lucas to access all the integrated services without having to log in again.

- **Browsing the product catalog:** With his token, Lucas was redirected back to the Product Catalogue Service, one of the Service Providers. He browsed through various laptops, read reviews and compared prices. Finding the perfect laptop, he added it to his basket.

- **Placing an order:** Lucas then accessed the Order Management Service, another Service Provider, to complete his purchase. Thanks to the token issued by the Identity Provider, he was automatically authenticated in the Order Management Service. Lucas reviewed his order, entered his shipping details and placed the order.

- **Needing service:** Later, Lucas realized he had a question about his order. He accessed the Customer Support Service, another Service Provider, via the platform. The service recognised his token, and he was connected to a support agent without having to log in again. The agent answered his questions, ensuring that Lucas felt confident about his purchase.

This case shows how Lucas was able to authenticate once with the Identity Provider (Shopping Platform Account System) and access various services (Product Catalog Service, Order Management Service and Customer Support Service) of an online shopping platform in a fluid way, taking advantage of the federated identity model, in which there is interaction between the identity provider and the trusted agents who provide the service.

Faced with the limitations of centralized and federated systems, especially in view of the role of the identified person, other structures have been debated. One example is the **identity structure centered on the identified person**. In this model, several service providers can share a single identity provider. However, there is no need to establish a notion of trust between the entities.

Whenever a person tries to access a service provider, they are routed to the requested identity provider, where they authenticate. The identity provider then releases the user's identity data to the service provider, where an authorisation decision is made based on the user's profile to grant or reject the request to access the service. With the absence of any notion of trust between service providers, all entities in this model implement the link informed by the identity provider.

Relying on the identity provider

Joana is a patient who needs to access various health services, such as medical appointments, laboratory tests and a pharmacy. Each of these services is provided by a different organization, but they all share the same identity provider, called SaúdeID.

Joana decides to book an appointment with her doctor via the online appointment portal. When she tries to access the portal, she is redirected to SaúdeID, where she had already registered, and logs in using her credentials (username and password). After successful authentication, SaúdeID releases Joana's identity data (such as name, date of birth, health insurance plan, relevant medical history) according to a specific profile, and sends this information back to the consultation portal. SaúdeID shares the personal information of data subjects depending on the requesting organization and the context in which the request is made. The consultation portal receives Joana's data and checks that she has the profile required to access the appointment booking service. Based on this information, the portal authorizes Joana to book her appointment.

Later, Joana needs to book a blood test. On accessing the laboratory's website, she is again redirected to SaúdeID for authentication. After logging in, SaúdeID releases the necessary data to the laboratory, which authorizes Joana to book the test.

Joana also needs to buy prescription drugs. When she enters the pharmacy's website, she is redirected to SaúdeID for authentication. After logging in, SaúdeID releases the necessary data (such as the prescription) to the pharmacy, which then allows Joana to buy the medicines online.

In this structure, each of the health services (consultation portal, laboratory and pharmacy) implicitly trusts SaúdeID to provide accurate and valid user identity and profile data. There is no need to establish explicit trust relationships between each health service, they all trust that SaúdeID is operating correctly.

Another structure is **decentralized** identity, also known as self-sovereign identity. Here, people have power over their own identity data and can selectively share it with trusted parties without relying on a central authority.

This structure presupposes not only the interoperability of a person's identity across multiple locations and service providers, with the user's consent, but also true user control over that identity, creating autonomy for the person. To achieve this, a self-sovereign identity must be transportable, it cannot be tied to one provider or location, and it must allow the person to choose when they want to disclose identity data to a third party, what data they want to share, to which entity, and for what purpose[46].

In the decentralized structure, once the user has consented to access, the verifier can directly authenticate the digital identities or credentials in the technological infrastructure - blockchain, for example - without involving the identity provider. This eliminates the need for the verifier to interact with the provider whenever verification is required. This is particularly useful when the provider no longer exists at the time of verification[47].

To realize these elements, decentralized systems generally use blockchain technologies, a type of *distributed ledger*, to enable the secure, peer-to-peer exchange of verifiable credentials. This is because the characteristics of the structures are similar. The blockchain essentially provides a decentralized domain that is not controlled

[46] ALLEN, Christopher. **The Path to Self-Sovereign Identity**. 2016. Available at: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html. Accessed on: 28 June 2024.

[47] PUNIA, Swati, *et al.* **Mapping the Blockchain Ecosystem in India and Australia: Case Studies**. 2023, p. 14. Available at: https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/final-blockchain-phase-2-report-for-printing-2023---pages-sequence-510.pdf Accessed on: 28 June 2024.

by any individual entity. The data stored on any blockchain is readily available (availability property) to any authorized entity (access property)[48]. Given these characteristics, a decentralized identity structure is linked to distributed registry tools.

Although distributed registration is one of the main topics of the decentralized structure, this solution can also be used in other structures, including centralized or federated ones, depending on the purpose. For example, blockchain technology is being used to issue the CIN, even though there is only one authority that fulfills the role of identity provider[49]. In this case, the blockchain assists in the consultation, enrolment and alteration of CPFs to avoid altered data and duplicate identities for the same person.

This structure seeks to put people, rather than identification authorities, providers or trusted parties, in control and at the center of identity transactions. In this system, it is possible for identity checks to take place without sharing the data itself, but only the confirmation that the relying parties must check. So, for example, to check whether a person is over 18, the relying party doesn't need to know the exact age or date of birth of the person identified, but only whether they are over 18.

Trential na Índia

The company has developed and implemented a blockchain-based verifiable credentials ecosystem that empowers citizens to have control over their credentials and enables the sharing of credentials data while preserving privacy.

Trential's solution includes a credential manager (an application for organizations to create, manage, issue and verify trusted identity data) and a wallet (a secure way for citizens to receive, store and share all their digital credentials in a single application). Trential has implemented blockchain to develop an immutable and verifiable data record that contains metadata related to credentials. This

[48] FERDOUS, Md Sadek; CHOWDHURY, Farida; ALASSAFI, Madini. **In Search of Self-Sovereign Identity Leveraging Blockchain Technology**. IEEE Access, v. 7, 2019. Available at: https://ieeexplore.ieee.org/document/8776589. Accessed on: 28 June 2024.

[49] BRASIL. Serpro. **Government starts using blockchain to issue the National Identity Card**. 2023. Available at: https://www.serpro.gov.br/menu/noticias/noticias-2023/blockchain-emissao-cin. Accessed on: 28 June 2024.

guarantees the integrity of the credentials, making them tamper-proof and allowing proof of credentials to be shared in a non-transferable way.

As part of the solution, a register of IIT Kanpur University students' diplomas was created, and this database was integrated into the Trential ecosystem. This made it possible for third parties to verify students' diplomas by simply scanning a QR code. Each diploma is linked exclusively to its credentials on the blockchain[50].

3.3 Purposes of the system

Another framework for identity systems is related to their functions, which are traditionally divided into two: a foundational purpose and a functional purpose.

A foundational, or legal, identity system aims to provide a unique and universal identity for people, meaning that anyone could be identified in any space by an element that only that person has. This system is known as foundational because it is used as a base, a foundation, by other agents for other systems and purposes. At the same time, this system is legal, since it is also one that is legally recognised by some rule or regulation as a way of guaranteeing that a person is a subject of rights before a state, a jurisdiction.

As described in the previous topic, legal identity is used for official state purposes, so that it is a recognition directly linked to the state that issues it. Furthermore, in view of its centrality to guaranteeing rights and duties, one of the UN's objectives, set out in Agenda 2030, is to provide legal identity for all people.

As a rule, these systems are made up of public registers such as civil registers, identities and population registers, which are created to provide identification to the general population for various types of transactions. An identity system can be considered foundational to the extent that it allows a person to prove who they are by using credentials recognised by law or regulation as proof of their legal identity[51]. As

[50] PUNIA, Swati, *et al.* **Mapping the Blockchain Ecosystem in India and Australia: Case Studies**. 2023, p. 15. Available at: https://ccgdelhi.s3.ap-south-1.amazonaws.com/uploads/final-blockchain-phase-2-report-for-printing-2023---pages-sequence-510.pdf Accessed on: 28 June 2024.

[51] WORLD BANK. **ID4D Practitioner's Guide: Version 1.0**. Washington: World Bank License, out. 2019, p. 12. Available at: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf. Accessed on: 28 January 2024.

a consequence, it is common for foundational identities to be developed and implemented by a country's public authorities.

!

Possible reasons for the development of identity systems

"Historically, the registration and identification of people by the state took place to facilitate the collection of taxes and to ensure that state benefits were received by the citizens. The control of the population through the use of identification has differed over time, but it is certain that the demand for identity documents is commonplace in the modern world[52]. Specifically with regard to digital civil identity systems, the political economy perspective behind the development of a security industry highlights the investment in digital identity systems following the 11 September 2001 attack in the USA[53]. In addition to this vision of an identity system for the preservation of national security, an agenda has emerged worldwide for the dissemination of identity systems for socio-economic development, especially with a focus on the world's poorest countries and regions, where there is still a significant proportion of people without civil registration"[54].

It is from this register of unique and reliable identities that the foundational identity system can become the foundation for secure identity verification for government and private sector users. On the basis of this system, authorities can understand the integrity of the identity proofing process, as well as being able to identify duplicates in other identity systems, such as an income transfer register or public payroll. From a foundational system, it is possible to reduce cases of fraud[55].

[52] LYON, David. **Identifying citizens: ID Cards as Surveillance**. Cambridge: Polity Press, 2009.

[53] LYON, David. **Identifying citizens: ID Cards as Surveillance**. Cambridge: Polity Press, 2009.

[54] MARTIN, Aaron. **Aadhaar in a Box? Legitimizing Digital Identity in Times of Crisis**. Surveillance & Society, [s.l.], v.19, n.1, p. 104-108, 5 mar. 2021. Available at: https://doi.org/10.24908/ss.v19i1.14547. Accessed on: 10 May 2022.

[55] WORLD BANK. **ID4D Practitioner's Guide: Version 1.0**. Washington: World Bank License, out. 2019, p. 15. Available at: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf. Accessed on: 28 January 2024.

New National Identity Card (CIN)

The CIN is Brazil's new foundational identity document. It has the CPF as its unique number, which, with an official flow of issuance and identification data throughout the country, would be enough to stop the use of divergent information in citizen identification. One of the CIN's challenges would be precisely to tackle the fragmentation and insecurity of civil identification systems, the various legal and infra-legal regulations, and the lack of a national standard for verifying the person. The CIN has a digital version, which can be accessed via the gov.br platform[56].

As a consequence of this foundational system, other systems are being coupled under the assumption that the foundational identity is universal and accessible to people. However, this understanding draws attention to a relevant risk: the exclusion of people who don't have any identity document from accessing public services.

Gov.br platform

Still on the subject of Brazil, the gov.br platform, linked to a foundational system, highlights this risk. This platform "uses the BDICN to authenticate its users based on a single login, so that citizens need to have their personal data catalogued in the BDICN in order to access public services digitized via gov.br. To do this, they need to have an identification document, which depends on the issue of a birth certificate - the Brazilian "founding document". Therefore, those who don't have this document are excluded from gov.br, and this slice of the population is more numerous in the North and Northeast regions. As a consequence, there is an imminent risk of exclusion from access to public rights and policies, such as social rights relating to labor and social security, such as the impossibility of issuing a Labour and Social Security Card (CTPS) and taking proof of life with the National Social Security Institute (INSS), both of which are constitutionally established as social rights"[57].

[56] BRAZIL. Digital Government. **Citizen identification and national identity card**. Available at: https://www.gov.br/governodigital/pt-br/identidade/identificacao-do-cidadao-e-carteira-de-identidade-nacional. Accessed on: 28 June 2024.

[57] BIONI, Bruno; GARROTE, Marina; MEIRA, Marina; PASCHOALINI, Nathan. **Between visibility and exclusion: mapping the risks of National Civil Identification and the use of its database for the gov.br platform**. Associação Data Privacy Brasil Research Association, 2022, p. 99.

A **functional** identity system, on the other hand, aims to issue and validate credentials used to authorize access to specific goods, rights and services, not general ones. A functional identity is not intended to be universal, since it has eligibility limited to certain sectors or purposes, which use identification processes to allow specific access.

Brazilian Driver's License

A common example is the National Driver's License issued by each state's Traffic Department (Detran), which, in theory, only certifies that a person is qualified to drive a car. The voter's license certifies that the holder can exercise their political rights, such as taking part in elections in their municipality, for example. However, people under the age of 16 cannot vote and therefore do not have voter ID in Brazil, which makes this document non-universal. The same is true of the CNH - only people who are authorized to drive vehicles can be identified by this system.

Not every person identified by a foundational identity, which is universal, has the same access to services, products and rights as people with a functional identity. In other words, not everyone with a foundational identity, such as the new CIN, can drive a car. At the same time, it is common for the functional identity to be based on the foundational one, like the CNH, where to issue it, you need to have a previous identity document[58].

Generally, public authorities create various functional identification systems to manage identification, authentication and authorisation for specific sectors or use cases, such as voting, taxation, social protection, travel, among others. This is the case in Brazil, where there are other types of identity, with personal data collected by a specific authority, such as the voter registration card, managed by the Electoral Justice, the CNH, issued by the Detrans, and the work and social security card, a document issued by the Ministry of Labour.

In some countries, particularly those without a foundational identification system, functional identity credentials are used as de facto proof of identity for purposes beyond their original scope. In the United States, for example, social security numbers

[58] FEDERAL DISTRICT. Detran. **Obtaining a National Driver's Licence**. Available at: https://www.df.gov.br/obtencao-de-carteira-nacional-de-habilitacao-cnh/. Accessed on: 28 June 2024.

and driver's licenses are issued as proof of authorisation for specific purposes, but are used as general-purpose credentials. However, functional identification systems are not normally considered legal identification systems unless they are officially recognised as serving that purpose[59].

!

But how do these frameworks work together? Government bodies, such as identification authorities, civil registrars, Ministries of Information Technology, Interior or Justice, are usually the main suppliers of basic identification systems. In addition, other government bodies, for example Ministries of Social Protection, Health, Education, Justice, Taxes, Customs, electoral administration, depend on these basic systems to interact with people or are themselves providers of functional identification systems. Finally, other government bodies play a regulatory role, supervise identification systems and may also be involved in implementing specific components or defining standards for technology and data formats[60].

Identity systems can also be used for **other purposes**, such as conducting identification processes to comply with *anti-money laundering* (AML), *customer due diligence* (CDD) or *know your customer* (KYC) regulations. It is common in these cases for the private sector to conduct functional identification processes and provide identifiers derived directly from foundational identities, i.e. official sources recognised by the Government[61].

Other identity systems are related to registration processes in physical spaces, social networks, shops, e-mail and e-commerce, for example. As a rule, the people identified declare some personal data and the identity organization collects other information, such as photos of the person's face and fingerprints. These systems do not necessarily use a legal identity to function, but it is possible that this identifier is collected.

[59] WORLD BANK. **ID4D Practitioner's Guide: Version 1.0**. Washington: World Bank License, out. 2019, p. 12. Available at: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf. Accessed on: 28 January 2024.

[60] WORLD BANK. **ID4D Practitioner's Guide: Version 1.0**. Washington: World Bank License, out. 2019, p. 12. Available at: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf. Accessed on: 28 January 2024.

[61] WORLD BANK. **ID4D Practitioner's Guide: Version 1.0**. Washington: World Bank License, out. 2019, p. 12. Available at: https://documents1.worldbank.org/curated/en/248371559325561562/pdf/ID4D-Practitioner-s-Guide.pdf. Accessed on: 28 January 2024.

Increasingly, however, these identity systems, especially those that serve non-foundational purposes, are putting pressure on the elements of a public infrastructure. Not necessarily every digital identity system is a DPI application. A public infrastructure aims to provide equitable access to digital services and infrastructure for all people, serving a public interest. At the same time, non-foundational systems, especially those operated by commercial entities, can prioritize specific customer segments or have access restrictions based on their business models, as well as identifying barriers in interoperability mechanisms, including for competitive reasons.

Furthermore, a fundamental aspect of DPI is the ability to integrate various digital services and components into a cohesive and interoperable ecosystem. Identity systems, however, may not have the interoperability or standardization required to integrate a wider DPI.

However, this does not mean that these systems do not somehow support the infrastructure. Increasingly, in order to guarantee validity in the identity verification process, which is fundamental to trusting the infrastructure, the service provider, the validating agent, uses multiple identity systems. The sum of these various identities, which may have been collected in different contexts, makes the process redundant and robust. This leads us to talk about not just one identity, but a layer of identities that together make up the user's identity, a topic that will be explored in the last section.

4 THE PURPOSES AND LAYERS OF IDENTITIES IN A DPI

This booklet has consolidated the idea that identity systems are fundamental for carrying out everyday activities. It is through a valid identity that people can prove who they are in a secure way and have access to rights, goods and services. Furthermore, based on a foundational identity, it is possible for other functional identity systems to be created to verify some attribute or characteristic of that already identified person, allowing for even more specific knowledge about them.

This identity agenda has been strongly promoted by the UN, the World Bank and the G20, through different approaches. The UN, with goal 16.9 of the SDGs, believes that all countries should provide a legal identity for people as a way of promoting peaceful and inclusive societies for sustainable development, providing access to justice and building effective, accountable and inclusive institutions at all levels. In order to achieve this goal, the World Bank believes it is essential to use registries that store personal data in digital format and credentials that rely on digital rather than physical mechanisms to authenticate people's identities[62].

From the discussions on DPI, the G20 has emphasized this infrastructure as a set of shared digital systems, developed and used by the public and private sectors. This infrastructure would be secure and resilient, built on open standards, enabling the provision of services at scale[63]. To this end, the secure flow of data, including personal and identity data, is recognised as a prerequisite for building this DPI.

However, identity systems carry a number of risks, which can vary in degree depending on their functionalities and frameworks. Taking into account the way they are structured and implemented, these systems can become tools of exclusion, discrimination and surveillance[64]. This is why governance, one of the pillars of DPI, is emphasized throughout the process of developing identity solutions.

[62] WORLD BANK. **World Development Report 2016: Digital Dividends**. Washington, 2016. Available at: https://documents1.worldbank.org/curated/en/896971468194972881/pdf/World-development-report-2016-digital-dividends.pdf. Accessed on: 28 June 2024. p. 194

[63] G20. **G20 New Delhi Leaders' Declaration**. Índia: 10 Sep. 2023, p. 22. Available at: https://www.mea.gov.in/Images/CPV/G20-New-Delhi-Leaders-Declaration.pdf. Accessed on: 28 June 2024.

[64] PRIVACY INTERNATIONAL. **The Sustainable Development Goals, Identity, and Privacy: Does their implementation risk human rights?** 2018. Available at: https://privacyinternational.org/long-read/2237/sustainable-development-goals-identity-and-privacy-does-their-implementation-risk. Accessed on: 28 June 2024.

One of the concerns raised by identity solutions is the difficulty of establishing adequate governance of the infrastructure and its applications, especially the data flow architecture, which is fundamental to its operation. As mentioned above, identity systems have different functions and can be organized in specific frameworks, depending on the agents involved, the structure of the system or the functionalities of the identity. These aspects translate into greater complexity for the operation of the system, which involves an intense flow of data in order to achieve different functions, as well as a greater number of agents involved and identifiable people, and possible applications in different contexts.

This complexification comes from the design of new frames for the systems, but also new layers of identity, in other words, the identification process cannot be understood as just verifying a person's identity, but as a process of disclosure of information between an identified person and an identifying agent. This disclosure can be as little as validating that the person really is who they say they are (by cross-checking biometrics, for example), to something more complex such as that the person is who they say they are and, based on other personal information or not, the financial transaction they carried out is not fraudulent.

These functionalities bring greater implications not only from a technological point of view, but also from a governance point of view. The DPI framework, in which these various forms of identification are interoperable and scalable, 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, with the potential to amplify risks.

Inferences based on identity elements

João works as a night security guard at a corporate building and, during his free time, uses his mobile phone to access his bank account statement via the bank's app. On a normal working night, he decides to make a financial transaction via the app. In order for the transaction to be carried out safely, the bank uses some information from the device, his transaction pattern and other personal information to detect any signs of fraud. However, this anti-fraud mechanism can harm specific groups, such as João, by using data that seeks to identify the person.

If data such as geolocation, place of residence (postcode) and mode of internet connection (mobile network or Wi-Fi) are used when defining this bank fraud indicator parameter and negatively affect a person making a financial transaction (increasing the chance of that transaction being flagged as potential fraud), people in vulnerable situations could be disproportionately affected. People who have no fixed address, or who work at night, or who live in outlying areas, and who only have access to the internet via a mobile connection will be more likely to be identified as potential fraudsters.

On its own, this increase in the propensity to identify fraud may not be an element that generates a significant impact for that person. However, by understanding identity from interconnected layers, these functional attributes can be used as parameters for other identification processes, such as in a background check process for employment, or a credit granting process, or anti-fraud verification in government assistance programmes. As a consequence, this initial marking of the banking anti-fraud system will have a cascading discriminatory effect on various other identification processes.

In this sense, the interoperability of different functional identity systems must be designed in such a way that **risks are not transmitted between different identification systems**. To this end, a participatory system of governance and auditing are essential elements in a digital identity arrangement in the context of digital public infrastructure.

The identity process conducted in layers is precisely the integration of multiple identity systems with their own levels of security and privacy. These layers can include basic digital identities for access to general public services, as well as more advanced and secure identities for financial transactions or access to sensitive or behavioral information. Thus, depending on the objectives of the system, what used to be identity frames are now understood as layers and these are now applicable together.

Layers of an identity with health information

1 João has an identity card in his name, identifying him with his biometrics, photo, full name, CPF, sex, date of birth, parentage, place of birth and nationality, as well as the issuing body and place of expiry of the identity card.

2 When João turns 18, he starts declaring his income tax. To file his income tax return, John registers on his country's government portal and authorizes the tax office to use his details to issue a pre-filled tax return.

3 When João loses his job, he registers on the government's social programme register as a requirement for receiving social assistance from the government. This registration is done through his government portal account.

4 When João opens an account with a bank in search of credit to start a business, he registers with the bank through the portal, which transmits only the essential information so that the bank can identify John and validate his identity and registration details. When he applies for a loan, João is denied credit. Some of the reasons for the denial are the fact that João is on the register for social programmes, 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 via the portal. João was unable to challenge the decision because there was no transparency mechanism to inform him of the reasons for the credit denial 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 work, and he is looking to formalize his enterprise with this loan.

5 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 lorry driver on this platform, the application process requests validation of identity through the portal, and asks for authorisation to access other data on the portal, including data relating to João's financial transactions, since the employer will be paying for the insurance on the lorry that João will be driving. João's application is rejected. The information regarding his registration on the social programme register and his credit score were determining factors in this decision.

> 6
>
> João returns to a situation of financial vulnerability and again applies to be included in the social assistance programme. When making this application, João is asked to send a high-quality photo of his face and his identity card. This is because the fraud detection system has 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. João's mobile phone has a broken camera and there are no face-to-face service points in the rural district where he lives.

The interoperability of information between the different layers that make up identification systems can amplify situations of discrimination against vulnerable populations and create new forms of discrimination. Therefore, when assessing the risks of an identity system in a DPI context, one must analyze both the risks inherent in the digitisation of identity, but also the risks that emerge from interoperability and facilitated data sharing on the same infrastructure.

Digital identities are now formed by the joining of layers, so that the end result is not just the joining of isolated systems dedicated to specific contexts, but links and inferences between these systems. The combination of these two risk-generating contexts can have consequences that are not merely the sum of the initial risks. An example of this is in layer 6, where a new discrimination arises. The inability of the user to authenticate correctly (a typical risk of digital identity systems) occurs because of the interoperability and excessive sharing of data in this infrastructure (a typical risk of digital public infrastructure systems).

The contextual element in the development and use of identity systems cannot be ignored in the face of the realization of data protection principles. Identity elements perceived in isolated contexts are being communicated to other identity layers, which can make it difficult for the holder to control and manage these identities.

In addition, behavioral information has come to make up identity. It is not only made up of information that a person records about themselves, but also information that emerges from their behavior. Metadata and records, as well as other forms of observed data, are generated from each interaction of the identified person.

The growing stores of data that companies and governments keep on individuals and groups are now generated automatically from human behavior[65]. Unbeknownst to people, their habits, preferences and choices are increasingly traceable and become part of their identity.

However, the convergence of these identities, or at least some of their attributes, in a digital system can create new challenges for the people identified, especially when it comes to their ability to develop their personality, be aware of the circulation of their identity information and exercise their autonomy.

There is an eminent risk of people being under constant surveillance by systems that identify them and add layers to their identity based on data observed or reported in a given context. In this scenario, even to carry out an everyday activity where identity validation is not necessary, identification systems are used to monitor people's behavior. In addition to surveillance and lack of autonomy, the way in which identity is perceived is also a risk, since all traceable elements of a person become classifiable, even if they are not recognised as valid categories by the system.

Classification of identity elements

Júlia is a non-binary person and is using a digital identity system to access a public service. The system asks her to declare herself as a woman or a man, but she doesn't fit into either category. By forcing her to choose between maintaining her full identity or accessing basic services, the system undermines her ability to navigate the world with autonomy and dignity. These artificial restrictions marginalise people, prevent them from participating in society and further classify them as "disabled". They also induce the collection of data that is not normally necessary for the system to function properly[66].

!

In a broader and more complex sense, identity is not just a set of biometric and biographical data. It is formed from a narrative constructed both by the person identified and by third parties who interact with and perceive that person. "The construction of personal identity involves a constant

[65] PRIVACY INTERNATIONAL. **Identities under our control**. Available at: https://privacyinternational.org/taxonomy/term/487. Accessed on: 28 June 2024.

[66] ACCESS NOW. **The Digital Identity Toolkit**. 2023. Available at: https://www.accessnow.org/guide/digital-id-toolkit/#mandatory-use. Accessed on: 28 June 2024.

process of selecting and interpreting personal information, giving rise to a dispute between different narratives from which identity emerges"[67]. As a consequence, depending on the information known and the capacity for self-determination, digital identification begins to impact on a person's way of being.

Furthermore, a lack of governance in the data used for identity systems can also lead to risks for people's rights to access essential services. Depending on how they are structured, it is possible for identity systems to act as barriers for those most in need. A person may be prevented from accessing services through the digital system because they lack meaningful access to technology, because they have specific attributes or experiences that prevent them from interacting easily with the system, or because the system exacerbates existing patterns of exclusion or disenfranchisement[68].

The immediate and aggravated damage caused by denying access to essential services such as banking, telecoms, energy, water, housing, health or education is almost immeasurable. People become more vulnerable to rights violations and abuses as a result of the digitisation of identity and the consequent processing of this data.

The governance of these systems is fundamental throughout the development and implementation process, so an unresponsive structure puts the system itself at risk. When designing an identification system, it is necessary to look at how it will be maintained and improved over time, as it is common for certain challenges to be realized only when the system is used. Therefore, it is not enough to develop tools to make the system implementable. Basic resources are needed to keep it working properly, without significant interruptions in access and so that it can be improved.

[67] MARTINS, Pedro Bastos Lobo. **The regulation of profiling in the general data protection law: the free development of personality in the face of algorithmic governmentality**. Dissertation (master's degree) - Federal University of Minas Gerais, Faculty of Law, 2021, p. 41. Available at: 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. Accessed on: 28 June 2024.

[68] ACCESS NOW. **The Digital Identity Toolkit**. 2023. Available at: https://www.accessnow.org/guide/digital-id-toolkit/#mandatory-use. Accessed on: 28 June 2024.

In view of these risks, identity systems must:

- Implement data protection as a fundamental principle, requiring the adoption of transparency approaches, specification of purpose and specific data sharing rules, always seeking to minimize such sharing;
- Seek approaches that prioritize people's power of agency[69], always guaranteeing their right to explanation and review of decisions made about them;
- Preventing the aggregation of data on a single centralized basis or the retention of unnecessary data, limiting the collection and use of personal data to protect people from data misuse;
- Introduce robust arrangements to ensure that the sharing of attributes and credentials takes place in a secure and traceable manner, and that the data is accurate, complete, kept up to date and relevant;
- Guarantee accountability tools for the agents involved in the development of systems, so that they take responsibility for their practices, especially those that impact vulnerable groups;
- Have participatory governance systems from the outset, guaranteeing the effective participation of the various stakeholders, especially civil society and vulnerable groups that may be particularly affected by digital identity systems.

Digital identity solutions, as one of the DPI applications, must fulfill the assumptions of an application based on open and interoperable technologies and developed on the basis of robust governance and multisectoral participation. Furthermore, a digital identity solution must be developed in compliance with the public interest, human rights and democratic values. This is a prerequisite for ensuring that the identity application complies with the parameters of a DPI. The risks arising from specific identity applications must be dealt with on the basis of these pillars in order to address their complexities.

[69] MARTINS, Pedro Bastos Lobo. **The regulation of profiling in the general data protection law: the free development of personality in the face of algorithmic governmentality**. Dissertation (master's degree) - Federal University of Minas Gerais, Faculty of Law, 2021, p. 41. Available at: 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. Accessed on: 28 June 2024.

DataPrivacyBR Research

APOIO

ripple