BETWEEN VISIBILITY AND EXCLUSION:

MAPPING THE RISKS ASSOCIATED WITH THE NATIONAL CIVIL IDENTIFICATION SYSTEM AND THE USAGE OF ITS DATABASE BY THE GOV.BR PLATFORM

DataPrivacyBR
Research

The Data Privacy Brasil Research Association is a non-profit civil-society organization that advocates for data protection and other fundamental rights in the context of the emergence of new technologies, social inequalities, and power asymmetries. The association's multidisciplinary team, drawn from various Brazilian regions is developing public-interest research, technical notes, texts analyzing emerging issues, workshops with decision-making agents, and society in general. The Association believes that data protection is one of the foundations of democracy and that it should be seen from the perspective of social justice and power asymmetries. It, therefore, works to promote a data protection culture and ensure that digital rights are fundamental rights for everyone, conducting publicly available surveys, guided by a strong social commitment and with ethical funding. For more details about the organization, the impact of its projects, and how its research is supported, visit www.dataprivacybr.org.

Press

For further explanations about the document or for interviews, contact the Association at imprensa@dataprivacybr.org

Authors

Bruno Bioni, Marina Garrote,
Marina Meira and Nathan Paschoalini

Revision

Thaís Aguiar

Design

Roberto Junior

This report is based on research funded by Open Society Foundations and was originally published in Portuguese. Financial support for the translation of this report into English was provided by Privacy International.

How to cite this document

BIONI, Bruno; GARROTE, Marina; MEIRA, Marina; PASCHOALINI, Nathan. Between visibility and exclusion: mapping the risks associated with the National Civil Identification System and the usage of its database by the gov.br platform. Associação Data Privacy Brasil de Pesquisa, 2022.

Summary

Executive Summary

The purpose of this policy paper is to analyze Brazil's National Civil Identification (or ICN), introduced by Law No. 13.444/2017, which is the main initiative centralizing the country's civil identification system, as well as the use of ICN's Database (BDICN) to authenticate users accessing public services on the federal government gov.br platform.

This report portrays a scenario of efforts undertaken nationally to implement a unified identification system, by different governments, for more than two decades. During this period, two legislative initiatives stood out: the Civil Identification Registry (RIC) introduced by Law No. 9.454/1997, however, it was never actually implemented, and the National Civil Identification (ICN), for which discussions ongoing since 2015 culminated in passing Law No. 13.444 in 2017. Both are based on similar information architectures, which tend to centralize the State's databases. In the case of the ICN Database, its structure is based on combining the TSE's biometric database with others from the National Civil Registry Information System, the National Civil Registry Information Center, the state government's and Federal District's Identification Institutes, and the National Identification Institute.

In addition to historically analyzing state government policy for the unification of the civil identification system in Brazil, this document covers the use of this national identification to access digitized public services, currently through gov.br, which is a federal government project to centralize its digital channels by gathering services and information about the work of every area of government. In this respect, creating gov.br is part of a worldwide trend toward platformed public services. According to Poell, Nieborg and van Dijck (2021), the platformization of society may be defined as the penetration of infrastructures, economic processes, and governance structures of digital platforms in different socioeconomic sectors, thus reorganizing cultural practices and social imaginary around these platforms.

The BDICN is currently used mostly to authenticate citizens accessing gov.br[1]. People wishing to use gov. br must have a single username consisting of their Individual Taxpayer Registration number (CPF) and a personal password. The ICN Database has been used to authenticate gov. br platform users accessing public services as of the Technical Coopera-

1 In February 2022, the TSE announced the next phase of the new National Civil Identification system: the National Identity Document, initially to be phased in for civil servants, then for the State of Minas Gerais, then for the entire population as February 2023 (TSE, 2022a).

tion Agreement signed on March 15, 2021, by the President's Office's General Secretariat, the Ministry for the Economy, and the Superior Electoral Court.

In a Brazilian context marked by profound socioeconomic and regional inequalities, formulating public policies to universalize civil registration and broaden access to public services - in other words, ensuring that all citizens are visible to the State - is essential. At the same time, if exacerbated, this visibility may lead to vigilante-type practices that are potentially discriminatory. Furthermore, international experience shows that initiatives to centralize civil identification systems may be conjoined with platformed public services to deepen exclusion for vulnerable people and groups rather than fulfill their stated intentions.

This policy paper is a contribution to this debate and to the efforts to develop and enhance public policies related to digital civil identification and the digitization of public services currently underway in Brazil, precisely studying the visibility-exclusion binomial. From the international and local literature, the report seeks to identify potential risks to the fundamental rights and civil liberties of citizens - or data subjects - that may arise from implementing National Civil Identification and using its database on gov.br in the context of Brazil's socioeconomic reality. Identified risks were divided into two groups: (i) abuse in processing personal data, related to ICN's information and governance architecture; and (ii) risk of excluding citizens from access to public policies; both risks are shown in the table below:

GROUP 1
Risk of abuse when processing personal data, related to ICN's information and governance architecture

Source of risk identified	Reason	Fundamental rights and civil liberties potentially violated by identified risks
Lack of plurality of views in the governance process for a complex public policy.	A non-multi-sectoral composition of a governance body, such as ICN's Management Committee and the Federal Executive Chamber for Citizen Identification (CEFIC) – the latter established by Decree No. 10.900/2021 –may fail to reflect the plurality of views required for the proper governance process of a public policy as complex as ICN and gov.br.	Potentially all of them - they cannot be delimited; ultimately governance choices will determine which rights and freedoms will be affected. In this respect, limiting society's participation could affect the Brazilian State's democratic regime.
Secondary and/or shared uses of personal data stored in ICN's database, in contrast to the principle of purpose limitation (article 6, I, LGPD)	There is a risk of abusive secondary use of personal data in ICN policy, which is particularly visible in four aspects: (i) the BDICN was set up by conjoining databases from other public spheres, whose purposes are not necessarily compatible with ICN policy; (ii) Using BDICN to authenticate users on the gov.br platform, which could mean deviating from the original purpose of ICN's data processing activities; (iii) Use of BDICN to cross-reference citizens' data in order to verify compliance with requirements for access to social benefits; (iv) Possibility of the Executive and Legislative Powers accessing the BDICN without any procedure for verifying their purpose of access.	(i) Violation of information self-determination, considered as a development of the fundamental right to personal data protection stipulated in the Federal Constitution's art. 5, LXXIX. (ii) Violation of human dignity, established as one of the foundations of the Federative Republic of Brazil, pursuant to the Federal Constitution's art. 1, III. (iii) Violation of the principle of non-discrimination, established as one of the foundations of the Federative Republic of Brazil, pursuant to the Federal Constitution's art. 3, IV, and the dignity of the human person as defined its art. 1, III. (iv) Violation of information self-determination, considered as a development of the fundamental right to personal data

		protection stipulated in the Federal Constitution's art. 5, LXXIX.
Discriminatory treatment of citizens and authoritarian practices	In addition to centralized information architecture, the ICN Database holds a huge diversity of data, including biometric data, which may enhance: (i) surveillance practices by the State; (ii) the unlawful exclusion of citizens from social assistance benefits based on discriminatory data processing, as per LICN Article 11.	(i) Mass surveillance has a chilling effect by lowering citizen participation in public spaces for fear of being watched by government, thus threatening the freedom of expression and assembly assured by art. 5th, IV, IX and XVI[2]. (ii) Discriminatory treatment puts equality at risk, which is guaranteed by the constitution's article 5, heading, item I, XLI, which determines with punishment any discriminatory practice harming an individual's fundamental rights and freedoms, as well as XLII, which defines racism as a crime, that is non-bailable and without a statutory period of limitation.
Violation of the data quality principle (article 6, V, LGPD)	According to the TSE there are some inconsistencies in the electoral biometric database: (i) In 2018, 9 million voters had a problem with immediate biometric identification during the elections. (ii) Since 2014, some 52,000 cases related to two or more identical biometrics have been identified.	(i) Impossibility of accessing public services via gov.br platform, access to public services is assured by the Constitution's art. 175. (ii) Difficulties when identifying voters to exercise the right to suffrage established by the Federal Constitution's art. 14.
Security incidents involving ICN Database	The BDICN holds (sensitive) biometric data for more than 110 million Brazilians, which amounts to large-scale data processing. A centralized information architecture becomes more likely to be targeted for	Violation of human dignity established as one of the foundations of the Federative Republic of Brazil, according to the Federal Constitution's art. 1, III. From the United Nations High Commissioner for Human Rights report,

2 For more details, see Article 19 (2021).

	severe security incidents since even a single episode could give access to a large amount and diversity of citizens' personal data, including sensitive data such as biometric data. In addition, security incidents involving biometric data reveal the even greater potential for harm, since these data are directly related to the data subject's body, so they cannot be altered.	August 2018 (A/HRC/39/29), "identity theft based on biometric data is extremely difficult to remediate and may severely affect an individual's rights."
Citizens' exercise of data subject rights stipulated by the LGPD	The gov.br platform, which uses the ICN Database to authenticate its users, as far as its interface and privacy policy are visible, does not have a direct and adequate communication channel enabling citizens to request confirmation of the existence of data processing, access to their processed data and rectification of incorrect or outdated data.	Violation of information self-determination, in its aspect of developing the fundamental right to personal data protection per the Federal Constitution's art. 5, LXXIX

GROUP 2
Risk of excluding citizens from access to public services

Source of risk identified	Reason	Fundamental rights and civil liberties potentially violated by identified risks
Exclusion of access to public services for people who do not have any identity document	BDICN to authenticate its users through a unique login, so to access digitized public services via gov.br, citizens must have their personal data cataloged in BDICN. To do so, they must have an identification document, which depends on a birth certificate to be issued - Brazil's "foundational document". Therefore, those not having this document are excluded from gov.br: this segment of the population is more numerous in the North and Northeast regions.	Exclusion of access to public rights and policies, such as social rights related to work and social security, for example the impossibility of issuing an Employment and Social Security Card CTPS) and of providing evidence of life for the National Insurance Institute (INSS), both constitutionally established as social rights by art. 6.
Exclusion of access to public services for people whose identity documents are in some way inadequate	The inadequacy of identity documents for trans people has the potential to exclude this population from accessing gov.br and, consequently, from public services accessed through the platform. This risk stems from the inexistence, in the ICN and in the gov.br portal, of a field for the inclusion of social name, so a person cannot be identified by the name they use and by which they are socially recognized.	Exclusion of access to public rights and policies, such as social rights related to work and social security, being unable to get an Employment and Social Security Card (CTPS) issued and provide evidence of life for the National Insurance Institute (INSS), both of which are constitutionally established as social rights in art. 6.
Exclusion from access to public services for hyper-vulnerable subjects such as children, adolescents, seniors, and people with disabilities	**Children and adolescent:** (i) Due to their age, their data have not been entered into the databases used (from the Electoral Courts and State Traffic Departments - DETRANs).	(i) Exercising rights and enjoying digital public policies and services being difficult or infeasible, thus violating the Child and Adolescent Statute's art. 3. (ii) Impossibility of exercising social rights related to the elderly,

	(ii) Since they do not possess biometric data registered with the BDICN, they may be unable to reach the maximum level of authentication, which is granted by biometric validation of the Electoral Court system data and data validation of digital certificates. **Seniors:** (i) Exclusion is associated with difficulties in using computers, cell phones, and the Internet resulting from illiteracy and functional illiteracy. **People with disabilities:** (i) The gov. br platform's authentication procedures are not accessible or inclusive for people with disabilities.	such as access to social security, established by the Federal Constitution's art. 6. (iii) Difficulty or impossibility of accessing digital public services, due to lack of accessibility, violating art. 4 of the Statute of Persons with Disabilities.
People being excluded from access to public services due to the absence or poor quality of Internet access	In this instance, the exclusion is brought on by the fact that citizens are unable to use the gov. br platform because they have partial or no Internet access at all. Recent data show that the absence of full Internet access is more often found among people from the most vulnerable social classes, who may even stop accessing public services due to a lack of connection.	Being excluded from access to public rights and policies such as social rights related to employment and social security or being unable to get an Employment and Social Security Card (CTPS) issued or provide evidence of life required by the National Social Insurance Institute (INSS), breaches constitutionally established social rights under art. 6.

By mapping the risks arising from implementing the ICN and using its database to authenticate users on the gov.br platform, this study concluded by highlighting the need for Data Protection Impact Assessment (DPIA) as stipulated by the Brazilian General Data Protection Law (LGPD). This recommendation considers that the data processing activities within the scope of the ICN and the use of the BDICN to authenticate users on the gov.br platform are high-risk operations for data subjects since high-volume personal

data processing touches on sensitive content such as biometric data. Hence the mandatory need for DPIAs for both public policies analyzed in this policy paper: National Civil Identification and use of the ICN Database to authenticate users on the gov.br platform[3].

On the federal level, the DPIA is still in the process of being regulated by the National Data Protection Authority (ANPD) and is due for the 2021-2022 biennium. However, official documents prepared by the Authority have pointed to criteria that pose a high risk for a given data processing activity, thus making a DPIA mandatory. This is the case of CD/ANPD Resolution No. 2 of January 2022, which states that large-scale data processing and the use of sensitive personal data, characteristic of both public policies here analyzed, are triggers for high-risk findings. Moreover, the "Guideline: application of the General Personal Data Protection Law (LGPD) by processing agents in the electoral context", prepared by the ANPD together with the Superior Electoral Court (TSE) in 2021, (TSE, 2021a) states that a DPIA must be produced in contexts that pose a high risk for personal data subjects, while also stating that producing a DPIA would be highly recommended in scenarios in which sensitive data were being processed on a large scale.

In addition to producing a DPIA, this policy paper analysis concludes that publicizing is mandatory because a DPIA is not a document for verifying a certain data processing activity's compliance, but a living document focused on the data subject's rights. It is basically a means of ensuring accountability for the protection of citizens' fundamental rights and civil liberties. In this respect, the duty of issuing and publishing a DPIA arises from both the purpose of the document itself but also from the constitutional principles of the Public Administration itself, especially the principle of publicity, which determines that its acts must be public and accessible to citizens.

3 TN: For the purposes of this translation, we have considered the "Relatório de Impacto à Proteção de Dados", in the Brazilian General Data Protection Legislation, the "Legislação Geral de Proteção de Dados" or "LGPD" as an equivalent to the "Data Protection Impact Assessment".

1. Introduction

1.1. Data Privacy Brasil Research Association and the Accountability and Digital Civil Identity project

Data Privacy Brasil is a space of intersection between the Data Privacy Education School and Data Privacy Brasil Research Association. The latter is a non-profit entity based in São Paulo that promotes personal data protection and other fundamental rights in the context of newly emerging technologies, social inequalities, and power asymmetries. Its multidisciplinary team from different Brazilian regions is developing research of public interest, technical notes, analyses of emerging issues, and training programs for decision-makers and society in general.

The Association believes that personal data protection is one of the cornerstones of democracy and it has to be seen from the point of view of social justice and power asymmetries. It, therefore, strives to promote a data protection culture and ensure that digital rights are fundamental rights for everyone while its ethically funded research is open to the public and guided by a strong social commitment.

This report, produced exclusively by the Association, presents the results of research conducted within the scope of the Accountability and Digital Civil Identity project (ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA, n.d a) funded by Open Society Foundations. Since June 2021, the project has been working to comprehend and map digital civil identity systems that are being developed and implemented in the Brazilian context. On this basis, the project helps to build a solid data protection culture and focuses specifically on governance and accountability measures, especially impact and risk assessments since these mechanisms are essential to assuring data subjects' fundamental rights and freedoms.

In other words, starting from a set of concerns for unequal and asymmetric relations between the State and individuals and considering the risk-benefits inherent to datafication processes, the project seeks to encourage reflection on better modeling of public policy for digital civil identity, which is key for the exercise of citizenship. In addition to posing and comprehending the obligation and the role of data protection impact assessments in the implementation of civil identification systems, this study undertakes a descriptive and evaluative analysis of how this State policy has developed over the last decade in Brazil. The guiding thread of the project, in this respect, is the framing of personal data protection as a central axis for the construction of a relationship of trust with less data-related asymmetry between the State and citizens.

Based on the project's objective, the Association has been involved in several activities such as exhibiting at the Turing Trustworthy Digital Identity Conference (ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA, n.d b) organized by the United Kingdom's Alan Turing Institute, and a workshop on data protection impact assessment and the public administration during the 2021 Innovation Week held by Brazil's Escola Superior de Administração Pública (ENAP) (DATA PRIVACY BRASIL, 2022).

As part of the project, the Association's team also held a closed workshop (ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA, n.d c) for the National Personal Data Protection Authority (ANPD), the Superior Electoral Court (TSE), and the Digital Government Secretariat (SGD), the main actors involved in both regulation for the data protection impact assessment and implementing Brazil's main digital identity system. The objective of this space for interaction, which was attended by Brazilian[4] and international experts from the Global North and South[5], was to foster debate around this important instrument established by the General Personal Data Protection Law (LGPD), especially on the mandatory requirement of impact assessment and its respective methodology considering the unique nature of data operations in the context of digital civil identity initiatives.

1.2. Between visibility and exclusion: mapping the risks associated with the National Civil Identification system and the usage of its database by the gov.br platform

As mentioned above, the purpose of this policy paper is to present the results of the research developed during the first year of the Accountability and Digital Civil Identity project. In this respect, the document analyzes, firstly, the National Civil Identification (ICN) established by Law 13.444/2017, since this is the main centralizing initiative of the Brazilian civil identification system. In addition, it also studies the use of the ICN system database for user authentication on the gov.br platform when accessing public services, which is the federal government's main website for materializing its digital transformation.

To perform an analysis of this nature, this study starts from the dilemma that citizens need to be known (IGO, 2018) and, to a certain extent, have to be datafied - or, ultimately,

4 The workshop on Brazil's impact assessment scenario and legislation was conducted by Isabela Maiolino, ANPD's regulatory coordinator, and Professor Maria Cecília Oliveira Gomes of Data Privacy Brasil.

5 In addition to Brazilian specialists, the workshop was attended by: Dariusz Kloza and Nikolaos Ioannidis, members of d.pia.lab research center affiliated to Vrije Universiteit Brussels (VUB).; Gabriela Zanfir-Fortuna, Kelsey Finch and Lee Matheson, members of the Future of Privacy Forum; Teki Akuetteh, Ghanaian researcher and director of Africa Digital Rights Hub4, and Carlos Guerrero, a Peruvian researcher at Instituto para la Sociedad de la Información y Cuarta Revolución Industrial.

surveilled - by the State in order to access public services and policies. So, a crossroads arises between the exercise of citizenship and surveillance, starting from the main ambition of data protection laws to affirm rights and duties for relations between data subjects and those who create them. This policy paper, therefore, asks which risks and benefits for fundamental rights and civil liberties may emerge from implementing a unified civil identification system and the use of digital identity as a mediator of access to digitized public services. From an extensive literature review supported by qualitative and deductive analysis, two main axes of analysis were posed: (i) risks-benefits related to the ICN's centralized information architecture; and (ii) risks related to the exclusion of citizens from access to public policies due to digitized public policies.

This report, therefore, hopes to help public authorities and other decision-makers with a reflection on network governance of risks identified in implementing the National Civil Identification and the use of its database for authenticating users on the gov. br platform. In addition to its stance in favor of the obligation to conduct and publicize a data protection impact assessment for this policy, the present study advances the discussion on the nature of the risks at stake and ways of effectively mobilizing the accountability tool stipulated by the General Data Protection Law.

This document is divided into six (6) chapters to address the main topics related to the development of a unified civil identification system, namely: Introduction (chapter 1); Unified National Civil Identity and Government Digitization: State Policies (Chapter 2); Risks of abuse in personal data processing: ICN's information architecture and personal data protection discipline (chapter 3); Risks of excluding citizens from access to public services on gov.br (chapter 4); addressing risks for fundamental rights and civil liberties: accountability measures and the Data Protection Impact Assessment(chapter 5); and, finally, its Conclusions (chapter 6).

Chapter 1 briefly conceptualizes the international scenario in terms of developing and implementing unified digital identity systems, at which point some of the problems associated with these systems that have been mapped in research from other countries will be noted. The second chapter details the history of the creation of a unique civil identification system and the context of digitization in Brazil. At this point, we will be revisiting some government digitization initiatives that culminated in the scenario in which Brazil is now situated.

Starting from this scenario, chapter 3 will scrutinize the National Civil Identification system's information architecture to describe the ICN Database's structure and this public policy's information flow, thus helping to identify any risk related to abuses in personal

data processing by this unified civil identification system. Chapter 4 will analyze the current use of the ICN Database to authenticate gov.br platform users and explore any risk of excluding citizens' access to services.

Having outlined risks - benefits arising from the ICN's centralized information architecture and the use of its database to authenticate users accessing public services, this policy paper concludes that the policy of using the BDICN for access to gov.br must be preceded by transparency and accountability instruments, in particular, a data protection impact assessment.

Chapter 5 critically addresses risk as a core component of the current grammar of personal data protection. Finally, Chapter 6 poses concrete recommendations on not only the need to compile DPIAs and publicize them when implementing public policies such as the ICN, but also the nature of the adverse effects at stake.

1.3. Digital civil identity, public policies, and surveillance

To situate the policy paper in the current discussion of digital civil identity systems around the world, a brief history of the most relevant previous reflections on this subject is required.

Historically, the State registered and identified individuals to facilitate tax collection and ensure that citizens received its benefits. Using identification to control the population has taken different forms over time, but demand for identity documents is certainly a commonplace in the modern world (LYON, 2009).

Specifically, in relation to civil digital identity systems, Lyon (2009) highlights the need for a political economy perspective behind the development of a security industry, which includes investing in digital identity systems in the aftermath of the 9/11 attack in the USA.

In addition to envisaging an identity system for national security purposes, a worldwide agenda has emerged that poses the dissemination of identity systems for socio-economic development, focusing especially on the world's poorest countries and regions, where a substantial portion of people don't have yet civil registration (MARTIN, 2021). Digital identity would therefore be the solution for registering this population and, consequently, a gate to access essential rights, as well as public services and policies for education, health, credit, assistance, and social protection (MASIERO, BAILUR, 2021).

However, the discourse for this potential advocated by the digital identity agenda for development has been confronted by experiences of citizens' rights violated during the practical application of these systems. This is what the academic literature points to - hence the importance of the implementation of digital identity systems as a topic of research (MASIERO, BAILUR, 2021).

In line with the digital identity agenda for development, an important point to note is that there are similarities between most digital identity systems that have been implemented in Global South countries. The civil society organization Access Now (SAWHNEY, CHIMA, AGGARWAL, 2021) uses the term "Big ID" for these systems: extensive identification programs promoted by the public sector or related to it, set up to assign each citizen a unique and ubiquitous digital identifier, store biometric and demographic data in a centralized database and authenticate identities through a centralized system, often using biometric authentication for this process. Indeed, a relevant factor in the development of digital identity systems and access to public services in low and middle-income countries is the proliferating use of biometrics. Meanwhile, in rich countries, biometrics is more often used for investigation and security purposes (GELB, CLARK, 2013).

Posing digital identity as a form of development in this way is aligned with the World Bank's Identification for Development (ID4D) initiative, whose aim is to provide access to services and promote the exercise of rights through digital identity. ID4D assumes that the implementation of digital identification is the right path to reach the UN Sustainable Development Agenda's goal 16.9 of providing legal identity for everybody by 2030, including birth certificates (WORLD BANK, 2022a). It is worth highlighting, as Martin (2021) emphasizes, that Sustainable Development Goal 16.9 does not mention the use of digital technologies, but the World Bank and other actors, especially in recent years, have joined the two agendas - providing legal identity and digitizing services and systems - on a specific political agenda. In this context, the World Bank works together with several countries to diagnose their identification systems and even fund new systems. In Brazil, the advancement of ID4D has so far been restricted to a report diagnosing the national identity system (WORLD BANK, 2022b).

Implementing digital identity systems in Global South countries immediately poses the question of citizens' personal data protection since a substantial portion of these countries either do not have data protection legislation or do not have a strong culture of consolidated personal data protection. India, for example, which has Aadhaar, the digital identity system most mentioned in the academic literature, launched it more than a decade ago and still does not have a data protection legislation (MARTIN, 2021). Therefore, we see a mismatch between digital identity systems posed as a development objec-

tive, which would be beneficial for citizens, and the legal infrastructure of the countries implementing them. In other words, there is a disparity between the needs and demands for visibility on the part of those who must be assisted by the State to access rights and services and a corresponding protective legal and institutional governance infrastructure. In this context, Martin (2021) highlights the need - in addition to legislation - for countries to have an effective regulatory capacity to protect personal data.

Kenya provides a recent example of the dialogue between protecting data and implementing a digital identity system. Kenya's digital identity system was created in January 2019. The process of collecting citizen data, including GPS and DNA, to feed the identity system began in March of the same year. Local data protection legislation was enacted in November 2019. After civil society organizations filed actions challenging the digital identity system in January 2020, the Kenyan High Court ruled that collecting GPS and DNA data was unconstitutional. Furthermore, the Court decided that continuing to implement the system and process data already obtained depended on compliance with legislation upholding constitutional values such as privacy. Despite this decision, the government continued to implement the system and civil society again filed an action to halt the effective use of the system until a data protection impact assessment had been compiled, as per Kenya's data protection legislation. Finally, in October 2021, the High Court of Kenya confirmed that a DPIA was required before implementing the system (OPEN SOCIETY FOUNDATIONS, 2022; NATION, 2021).

As it was in Kenya, the development of digital identity solutions worldwide was spurred by the Covid-19 pandemic, given its inherent characteristic of allowing business transactions and social assistance measures to proceed while individuals remained socially isolated, and because these initiatives are associated with proposals for immunization and vaccination certificates (MARTIN, 2021). Africa and Asian countries, in particular, after the outbreak of the pandemic, in some cases with financial support from the World Bank, started to implement digital national identity systems using MOSIP, an open-source platform based on India's Aadhaar digital identity system, funded by the Bill and Melinda Gates Foundation, Sir Ratan Tata Trust and Omidyar Network (MARTIN, 2021). The same trend has been seen in Brazil, where the use of the ICN Database to access gov.br was introduced during the pandemic when gov.br accesses and user numbers grew dramatically. The total number of Brazilians using gov.br services grew from 1.7 million in January 2019 to 113 million in September 2021 to then reach 130 million users in June 2022, which corresponds to 80% of Brazilians aged 18 or more (CÂMARA DOS DEPUTADOS, 2021, GOVERNO FEDERAL, 2022c).

From collecting taxes to accessing public services and policies and on to the battle to beat

the pandemic, there is historically interdependence between surveillance and identification of the citizen by the State. For their interactions with the State, citizens must be visible (IGO, 2018). Their identification - and their cataloging too – are key to entering the state's bureaucracy. This relationship, given the trend toward state-of-the-art digital civil identity systems worldwide, poses two reflections, which, to a certain extent, will permeate this entire study.

The first relates to the rise of personal data protection laws and their connection to the State's demand to know more about its citizens to formulate public policies (MAYER-SCHÖNBERGER, 1997). Data protection laws empower several actors in addition to citizens that are empowered as data subjects. These other actors are called data processing agents since they too have agency over these bits of information. For example, as we shall show below, they have the prerogative of manipulating data regardless of any need to obtain data subjects' consent in certain cases. The law, therefore, is not a neutral element in the correlation of forces between watchers and watched. The contentious question here is how legal-institutional governance arrangements for civil identity and data protection systems may be mobilized to diminish power asymmetries between these two poles - State and citizens.

The second reflection is that surveillance is in some way accepted when combined with the welfare state. By mapping literature in this field and using qualitative empirical studies of public perception of privacy threats, Nathalie Maréchal (2015) shows how little attention is paid to this so that there is almost no pushback against State surveillance on the pretext of aiding those being watched. In other words, the practices, and the concept of surveillance itself are paradoxically less visible when citizens are more visible and watched.

In this respect too, Murakami Wood and Firmino (2009) investigated people's opinions of a new single national identity system in Brazil and found that most responses were favorable. The researchers interviewed community leaders, human rights activists, and members of the police from across the political spectrum. Most thought that the system would be a guarantee against anonymity, which in turn would give rise to abuse by the State or other malicious persons. The identity system, in this sense, was not seen as a means of State intrusion or control. In other words, in this relationship of interdependence between surveillance and identification, Brazilians were more concerned to be identified - in the sense of being visible. A point that must be considered, therefore, in terms of the situation in Brazil, is that citizens feel a need for visibility to access public policies, while not ignoring the need to protect their data, especially from the most vulnerable individuals who depend most - and more often - on public policies and are therefore found in state databases.

Starting from this complex relationship between surveillance and identification, this policy paper analyzes the issue of digital civil identification not as an end, but as a mediator of the relationship between the State and citizens for access to services and public policies. Masiero and Shakti (2020), in this understanding of digital civil identification as a mediator of the State-citizen relationship, outline three theoretical perspectives for India's digital identity system, proposing an integrated and non-exclusive analysis of its functions. The first view is that of Aadhaar as a means of data identification for citizens and, from then on, a determinant of their eligibility for access to public policies. The second is from Aadhaar as a platform that has a foundation - the citizens' database - and coupled to it are public services, built on that foundation. Finally, the third perspective outlined by the authors is Aadhaar as a form of mediated surveillance, in which surveillance is not only exercised by the State, which owns the database, but also by all entities that have access to or may use its data. So in addition to centralized and state surveillance architecture, the model would involve far-reaching decentralized surveillance[6].

Transposing this theoretical proposal to the use of the BDICN to authenticate citizens on the gov.br (the Brazilian case analyzed here), one may find that citizens are being datafied precisely by the ICN Database. Moreover, under Brazil's Civil Identification Law (LICN), art. 11, ICN's information may be used to decide whether citizens are eligible for public policies. Secondly, by turning this database into a means of authenticating gov.br users, a series of services are attached to a foundational structure – as of now all of them are public services, but the BDICN has also been used to authenticate consumers connecting to services such as online banking. Finally, the ICN may also be analyzed from the point of view of facilitating mediated surveillance, since public administration entities get wide-reaching access to its information and secondary use of its data, an aspect to be discussed in more depth in Chapter 3 of this policy paper.

The application of Masiero and Shakti's (2020) analytical model for Aadhaar in the Brazilian case, as well as the descriptions of how digital civil identity systems have been implemented in similar ways in Global South countries, with the same socioeconomic

6 The "Viral Data" report found higher percentages of private actors of Brazilian origin acting in the supply and development of technologies to combat Covid-19 for the public sector by using personal data, in around 53.84% of cases the public sector did not pay for the use of the technology. The survey highlights characteristics t to be watched for relations between public and private sectors in the provision of technology for essential public services. Firstly, although the technology was provided free of charge during the pandemic, it may become an essential part of a public service and part of a paid service, thus creating a situation in which providing public services would depend on private companies. In addition, an important issue to verify is how datafied public policies may lead to the State being more dependent on the private sector, in which case the latter gains access to extremely substantial citizens' databases, then a crucial need arises to determine who is part of the data processing chain, who the agents are and which country they are from, whether there is the international transference of data.

development discourse, are important as far as they emphasize that the analysis in this report is not limited to Brazil. Although Brazil's case is the one analyzed herein, the points made may be transposed to other countries and international discussions.

2. Unified national civil identity and digitization of the government: State policies

2.1. Civil Identification Registry

Doneda and Kanashiro (2010) place Brazil on a list of countries that have introduced decentralized identification systems. Since there is no communication between the registration systems used by the General Registry - or RG - one single citizen may have more than one identity card, each bearing different identification numbers issued by different state governments (DONEDA, KANASHIRO, 2010). In this context, a proposal has emerged for Brazil to develop a single identity system enabling a higher level of authenticity in the face of several cases of fraud, given that ID documents are easily copied.

The history of this initiative for a single identity dates back to the 1990s - more specifically 1997 - when President Fernando Henrique Cardoso's federal government promulgated Law 9.454/1997 establishing the Civil Identification Registry (RIC) to replace Brazil's Identity Card (RG). Doneda and Kanashiro (2010) note that this new system stipulated the use of unique numbers identifying all Brazilian citizens, to mediate all their relationships, whether public or private.

In order to fulfill its objective of becoming a single civil identification document, the RIC proposal was based on an architecture that concentrated several other identification documents: the identity card (RG), National Driver's License (CNH), Individual Taxpayer Registry number (CPF), voter registration card, Employment and Social Security Card (CTPS), individual registration in civil servants' Social Integration and Savings Programs (PIS/PASEP) and their registration number for the National Institute of Social Security (INSS) (KANASHIRO, DONEDA, 2012). This concentration of information in a single document would therefore lead to several databases being merged.

Law No. 9.454/1997 came into effect at the time of its publication, but its art. 5 stipulated the need for supplementary regulations, which should have been added within one hundred and eighty (180) days, to be subsequently implemented within 360 days. Although regulatory supplements for the RIC were not added until 2010, 13 years later, when Decree nº 7.166/2010 was published, the implementation of RIC began earlier in 2004, when the equipment was acquired to digitize the biometric identification data that had been part of Brazilian ID cards (locally RGs) (KANASHIRO, DONEDA, 2012). Once regulations had been drafted for the RIC, work started on procedures used to in fact implement this new

identification system. The Ministry of Justice (SE/MJ) through its Executive Secretariat was in charge of the RIC project, which involved signing a 'technical cooperation agreement' between the Ministry of Justice and Universidade de Brasília in order to conduct research into processes and infrastructure required for the new Civil Identity Registry. In this context, a series of technical reports (Ministério da Justiça e Segurança Pública, n.d) were produced to support the federal government's decision-making processes in relation to the public policy.

In 2015, when Draft Law No. 1775/2015 called for another single civil identification system, to be known as the National Civil Registry (RCN) - subsequently voted under a different name: "National Civil Identification" (ICN), all activities related to the RIC's implementation were shut down.

Despite efforts undertaken to write the best possible RIC draft law, it was never actually implemented. As Kang, Doneda, and Santos (2016) note, the reasons for not being implemented were probably cost-related.

2.2. National Civil Identification

As mentioned above, Draft Law 1775/2015 posed a new unique civil identification system - the National Civil Registry (RCN) - which would revoke the Civil Identity Registry (RIC)[7]. On the initiative of the federal government together with the Electoral Court, a draft law creating the RCN was signed and submitted by the then Justice Minister and the Minister of the Small and Medium Business Secretariat - José Eduardo Cardoso and Guilherme Afiff Domingos respectively.

The draft law sought to create a national civil registry together with a national identification document, which would enable a simplified but more secure relationship between citizens and public and private entities (KANG, DONEDA, SANTOS, 2016).

According to Kang, Doneda and Santos (2016), to fulfill its purpose, the draft law called for the creation of a new database to be built by merging the Electoral Court's biometric database with the National Civil Registry Information System (SIRC), in addition to other data not found in the SIRC but available in databases used by the Electoral Court or other public entities.

7 While PL 1775/2015 was being discussed in the Chamber of Deputies, the article that revoked the RIC was withdrawn, so the law that established the Civil Identity Registry is still in force today, although its implementation is suspended.

Several public hearings were held while the draft law was going through the Chamber of Deputies in 2016. There were 16 technical meetings in total, and attendees were predominantly from congress, although other interested sectors took part too. But there was very little civil society involvement in the public hearings: only two representatives were present in the meetings (KANG, LUCIANO, and SANTOS, 2017).

Once technical meetings had been held and amendments to the draft law taken, its rapporteur deputy Júlio Lopes submitted some substantial alterations to the text as originally drafted (KANG, LUCIANO, 2017). By 2017, draft law No. 1.775/2015 had been voted by a Chamber of Deputies plenary session and re-named Supplementary Draft Law 19/2017 to be discussed in the Senate.

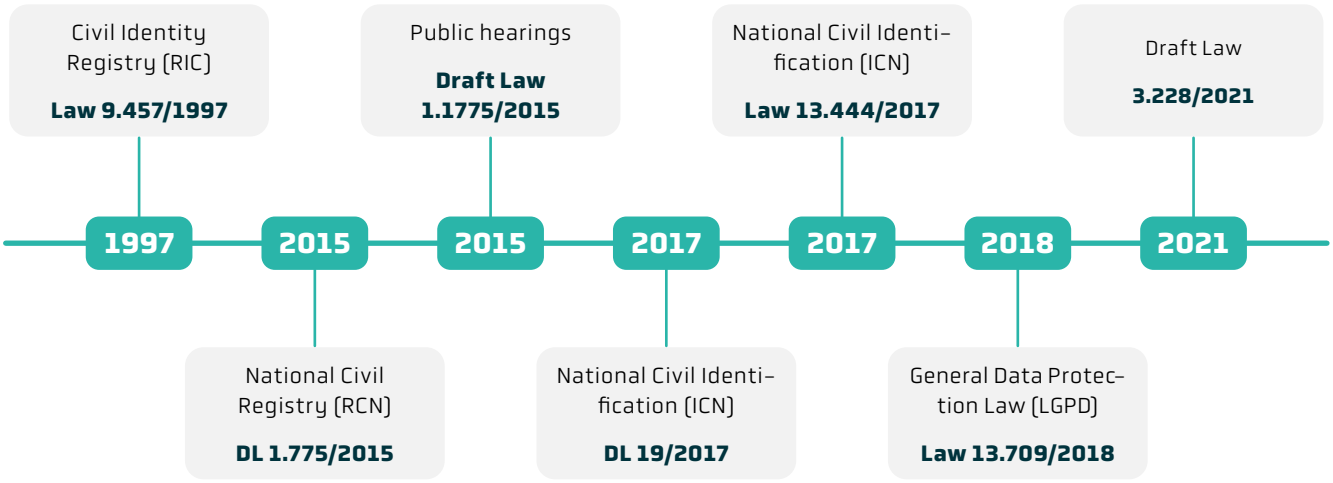
As of this time, Supplementary Draft Law No. 19/2017 called for the creation of a National Civil Identification (ICN)[8]. Finally, before the end of 2017, the draft law was voted by the Senate and sanctioned by then President Michel Temer: Law 13.444/2017 (or LICN) was promulgated. So, the ICN formally came into existence as a system based on centralized information architecture inherited from previous initiatives such as the RIC, mostly consisting of biometric data from the Electoral Court's database.

The LICN was voted, and efforts were made to ensure that the National Civil Identification system would be implemented. These efforts were stepped up in 2018, when President Jair Bolsonaro was elected and headed an administration that has prioritized the Brazilian government's digital transformation, as shown by the Digital Government Secretariat's digitizing more public services (GOVERNO FEDERAL, 2022) and the placement of Draft Law 3228/2021, altering the ICN Law, as a legislative priority for 2022 (BRASIL, 2022).

Also, in relation to efforts made to implement the ICN, it is worth noting the contract signed by the Electoral Court and the Federal Data Processing Service (SERPRO) in December 2021 (TSE, 2021e). This instrument states that Serpro will be responsible for the operation of the ICN system, from providing biographical and biometric identification services and biographical research to issuing National Identification Documents (DNIs), for a period of five years (LOBO, 2022).

8 According to Kang and Luciano (2017), the identification system's nomenclature was changed after the acceptance of the amendment to the bill seeking to amend art. 1 of Draft Law 1775/2015. The amendment alters the new identification system's name, since the civil registry is constitutionally a private entity, therefore its attribution to the public authorities – in this case the Electoral Court – is unconstitutional.

The timeline shown below outlines the main legislative initiatives mentioned in this section to finally set up a unique civil identity system:



This reconstructed timeline shows that developing a unified civil identity system has occupied practically all governments of differing ideological origins since Brazil reinstated a democratic regime. Introducing a system of this type may therefore be posed as a long-standing State policy, while at the same time it is still in progress.

2.3. A brief history of Brazil's digital transformation

Initiatives undertaken to develop a unique civil identity system have been directly linked to Brazil's digital transformation processes that started in 2000, when the Electronic Government Policy Proposal for the Executive Branch was voted, followed by its journey toward digital government (THORSTENSEN, ZUCHIERI, 2020).

Although several government digitization initiatives have been initialized over the last two decades, it was only in 2016 that a more solid strategy was established to develop digital government: the Digital Governance Strategy (locally EGD). This policy combined with an interest in moving from e-government to a digital government structure[9] called

9 According to the Ministry for the Economy's website (2019), the 'electronic government' notion evolved together with Information and Communication Technologies (ICTs), particularly the Internet, which reshaped relationships between Public Administration and society. Several separate initiatives were identified in which Brazilian citizens were offered public services virtually, such as delivering income tax returns. However, there was a still-deficient infrastructure consisting of several separately managed networks, so the services offered did not meet "performance and interactivity standards,

for a series of frameworks and structures to steer digitization-related programs and actions (OECD, 2020).

Two years later, in 2018, Digital Governance Strategy underwent a series of updates that sought to define certain priorities related to (i) boosting the use of digital technologies for transparency; (ii) improving digital services; (iii) ensuring the implementation of digital identity systems; and (iv) integrating digital services through the implementation of information technologies, systems, and interoperable data to grow public participation using digital platforms (OECD, 2020).

By the time this strategy ended, after lasting from 2016 through 2019, a new document of this type was published, for the 2020 - 2022 period. It was named Digital Government Strategy (Decree No. 10.332, of April 28, 2020) and its goal is to have all federal government services digitally offered through the gov. br platform. Law No. 14.129/2021 was voted to ensure its feasibility with rules, principles, and instruments for the Digital Government and to boost the public administration's efficiency.

By altering social dynamics and requiring social isolation as a public health measure, the Covid-19 pandemic and its context accelerated the federal government's digital transformation. Data from Agência Brasil in November 2021 showed that about 72% of public services offered by the Federal Executive Branch had been adapted and were ready to be offered through digital platforms (AGÊNCIA BRASIL, 2021). On the same note, the federal government estimates that all federal public services will have been digitized by 2022, as may be seen in Decree No. 10.996 of March 14, 2022, which alters the Digital Government Strategy.

Nevertheless, note that the government digitization process does not amount to a positive development per se. A recent report posted on the Telesíntese website (2021) featured a speech made by Federal Audit Court judge Aroldo Cedraz, who referred to the fact that a country's digital transformation should not be limited to digitizing public services: the whole society must be part of this process. Along the same lines, the vote proffered by Rapporteur Judge Vital do Rêgo - in the context of a report monitoring the Digital Governance Strategy, produced by the Federal Audit Court in 2021 - noted that the absence

interfaces were not always user friendly and the various government agencies were mismatched in terms of their assimilation of ICT" (MINISTÉRIO DA ECONOMIA, 2019). Therefore e-government played a key role in computerizing the Public Administration's internal processes, but it had to shift its focus away from its internal processes to relations between Public Administration and Society. In this respect, the digital government initiative arises to simplify and make relations between citizens and public authorities more accessible and efficient in the provision of digital services for citizens (MINISTÉRIO DA ECONOMIA, 2019).

of a systemic approach to the digital transformation process could lead to limitations for digitally provided public services. Merely digitizing is not sufficient for the population to actually reap the benefits of digital transformation, which would require investing in infrastructure, connectivity, and citizens' digital literacy (TRIBUNAL DE CONTAS DA UNIÃO, 2021).

2.4. The gov.br platform

The gov.br platform emerged in 2019 after Decree No. 9.756/2019's publication. This initiative is based on one of the pillars of the Digital Government Strategy, which establishes the need to unify communication channels and access to digitalized public services.

The platform's home page states gov.br is at its beta stage of development, which means that the portal is still being improved and has not yet reached its final version. The federal government itself has stated that gov.br:

> is a project to unify the government's digital channels. But above all it is a project that shows what a citizen's relationship with the State should look like: uncomplicated and focused on the needs of people who use public services.
>
> It all starts with the gov.br portal, which shows services for citizens and information of actions taken by all areas of government in one place. By December 2020, the government's websites will be integrated so gov.br will be the only entrance to the federal administration's institutional pages, thus offering citizens a fast channel directly relating to federal agencies. (GOVERNO FEDERAL, undated, no pagination).

A fully functioning gov.br website depends on identification and authentication processes for users accessing the platform, one single username consisting of their Individual Taxpayer Registration number (CPF) and a personal password. All gov.br accounts involve three authentication levels - bronze, silver, and gold - relating to how these accounts were created and/or validated. According to the federal government (2021), the different levels, which are linked to user data validation security levels, ensure different types of access to digital public services and transactions that may be made via the gov. br platform. Brazilians using gov. br services numbered 1.7 million in January 2019 then rose to

113 million in September 2021 and reached 130 million users in June 2022, equivalent to 80% of Brazil's total number of citizens over 18 years old (CÂMARA DOS DEPUTADOS, 2021, GOVERNO FEDERAL, 2022c).

In order to strengthen the integrated national system for citizen identification and facilitate their access to services provided by the gov.br platform, a Technical Cooperation Agreement (ACT) signed by the President of the Republic's General Secretariat, the Ministry for the Economy and the Electoral Court addresses the use of the National Civil Identification (ICN) system in the context of the gov.br portal (TRIBUNAL SUPERIOR ELEITORAL, 2021). The ACT ensures the authentication of platform users by validating registrations with data comprising the ICN's Database - especially the Electoral Court's biometric database (TRIBUNAL SUPERIOR ELEITORAL, 2021).

The signing of this Technical Cooperation Agreement was one of the first moves toward effective implementation of the ICN[10], as far as it constitutes the main use of its database to date - its use for validating and authenticating users, with the Electoral Court's biometric database, ensures citizens' access to gold-level gov.br accounts and enables them to access all digital public services available on the platform.

The development of the gov.br platform is part of a broader movement observed internationally toward platformed public services, following a more general trend toward a platformed society. Poell, Nieborg and van Dijck (2021) suggest that the platformization of society may be defined as the penetration of infrastructures, economic processes, and governance structures of digital platforms in different socioeconomic sectors, which results in the reorganization of cultural practices and the social imaginary around these platforms. In this respect, van Dijck, Poell and De Wall (2018) argue that the inclusion of platforms in today's everyday life, by promoting an intensified collection of individuals' data, allows aspects of life that were not previously quantified to be datafied, such as data of behavioral profiles and location data.

Initially, observers could claim that this platformization phenomenon was mainly concentrated in the private sector, from where it originated. However, Dahl-Jørgensen and Parmiggiani (2020) point to the recent penetration of digital platforms in the public sector, which, in turn, corresponds to the development of digital infrastructures offering public services for citizens.

10 In February 2022, the TSE announced the next phase in the introduction of National Civil Identification. The National Identity Document is to be phased in for civil servants initially and then for the entire population of the State of Minas Gerais as of February 2023 (TSE, 2022a).

In this respect, Dahl-Jørgensen and Parmiggiani (2020) suggest that incorporating technical infrastructure belonging to large technology companies into public platforms is a common process that shows public and private sectors intertwining to develop technologies, resulting in a sectorial transgression[11] visible at other times, such as the development of technologies to combat Covid-19 (ANDRADE *et al.*, 2021). This transgression, the authors say, may impact citizens in terms of social inclusion and participation, since platforms act directly on citizens' ways of engaging with democratic decision-making processes and interacting with the public authorities (DAHL- JØRGENSEN, PARMIGGIANI, 2020).

Alongside gov.br, two examples of platformed public service help to illustrate the concept. The first of these is the UK's *National Health System* (NHS). Faulkner-Gurstein and Wyatt (2021) indicate that platform logic has gone on to permeate changes in the NHS's organizational objectives and strategies over the last 20 years. Its platformization has been posed both as open State policy, without setting an expiration date, and as a strategic pathway for future changes. In structural terms, the NHS collects and stores data on citizens who access it, which serves the purpose of facilitating and intermediating their access to services, and offers infrastructure and resources to support research, thus showing the centrality of data in the platformization process (FAULKNER-GURSTEIN AND WYATT, 2021).

The platformization component is also a prominent feature of India's digital identity system (Masiero and Shakti, 2020). As mentioned above, Aadhaar may be seen as a platform based on a citizen database with services attached such as integrating biometric identification for citizens' receiving government poverty alleviation program payments (MASIERO E SHAKTI, 2020).

11 Solano *et al* (2022) suggests that the notion of sectoral transgression may be seen as the involvement of commercial actors in spaces in which their business models, practices and ethical frameworks are out of step with the interests of other actors that shape public debate.

3. Risks of abuse in personal data processing: ICN's information architecture and personal data protection discipline

This chapter introduces the National Civil Identification system's information architecture and governance structure, as determined by Law 13.444/2017. From this description, convergences, and tensions between the LICN and LGPD will be identified, as will changes posed by Draft Law No. 3228/2021, which seeks to amend the LICN. Fundamental aspects addressed in this section include the correlation of centralized information architecture with a higher level of complexity for governance. In addition to addressing information security issues, this chapter also tackles controversial legal issues such as the possibility of secondary uses of ICN's personal data and its component databases.

3.1. Governance structure per the National Civil Identification Law

a. ICN Management Committee

By reading and analyzing the legal provisions established in the LICN, the existence of a governance body may be identified: the ICN's Management Committee (locally CGICN). Per the definitions in Law No 13.444/2017, art. 5, the CGICN consists exclusively of members of the public authorities, among them representatives of the federal government, the Superior Electoral Court, the Chamber of Deputies, the Federal Senate, and finally the National Council of Justice.

In terms of attributions, the CGICN has the competence to make recommendations on the biometric standard used by the civil identification system, the technical and economic-financial parameters of the biometric data verification service, and the guidelines for the administration of the National Civil Identification Fund and management of its resources. In addition, the CGICN may advise on the interoperability implemented across the federal Executive Branch and Electoral Court systems and may establish its own bylaws.

This Committee is therefore demarcated by governance arrangements that do not fit a multisectoral format. According to Almeida, Getschko and Afonso (2015), a multisectoral committee is one designed to bring together the main sectors interested in certain aspects of decision-making processes, based on democratic principles of transparency and participation. By bringing together various actors in society, such as government, the

private sector, academia, and civil society, the multisectoral model enables to extend the debate in the public sphere.

Considering the objective of implementing a single civil identity system - which is a public policy, that manages its own funds, and is based on a high volume of personal data processing - the fact that the ICN Management Committee is not multisectoral, in opposition to the Internet Management Committee (COMITÊ GESTOR DA INTERNET BRASIL, nd), the Committee for the Defense of Users of Telecommunications Services (AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES, 2021) and the National Personal Data Protection Council (AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, 2022), is not in line with the Brazilian experience of complex system governance, which has historically encouraged a wide range of sectors of society to participate in decision-making processes and advise on public policies, alongside the public sector.

Due to the governance arrangements for the ICN, there is a possibility of just one perspective predominating in decision-making processes – which could potentially and predominantly be guided by an idea of efficient provision of services and progressing the unique identification policy – to the detriment of protecting data subjects.

b. Draft Law Nº 3228/2021 and alterations in ICN's governance arrangement

In September 2021, the federal government had Draft Law Nº 3228/2021, amending the LICN, forwarded to congress, which reignited public discussion on implementing a digital civil identity (GARROTE *et al*, 2021a). The draft law poses certain changes in the structure of the ICN - including changes in its information architecture - to be discussed below.

Ranked one of the federal government's legislative priorities for 2022, according to ordinance No. 667/2022, the proposed text includes an amendment to the LICN's art. 5 paragraph 1, requiring the CGICN's membership to include a representative of the federative units (states) and the Federal District, to be appointed by the Minister of State for Justice and Public Security. Despite this proposed amendment, the new terms suggested in the draft retain an ICN Management Committee consisting exclusively of members of the government.

c. ICN Management Committee and Decree Nº 10.900/2021

In the wake of discussions on National Civil Identification's governance structure, in December 2021, the President published Decree No. 10.900/2021 on "Citizen Identification Service (SIC) and the governance of identification of natural persons in direct, autarchic and foundational federal public administration" (BRASIL, 2021a). This Citizen Identification service is delivered through the gov.br platform and publishing the decree fulfills the objective of regulating its use by public and private entities.

By instituting and regulating the Citizen Identification Service[12], the decree adds a new data processing operation to the ICN policy umbrella. This is because the citizen authentication process referred to in the decree mostly uses the National Civil Identification database, combined with the Citizen Base Registry and other databases that may be incorporated into the SIC. In other words, the legal text places the BDICN within an even broader information and governance structure.

The decree also establishes the Federal Executive Chamber for Citizen Identification (CEFIC) with powers to manage the Citizen Identification Service, including the use of the BDICN. On this basis, the creation of CEFIC is to some extent an alteration of ICN's governance arrangements since it leads to an even greater centralization process in relation to the current structure. In this case, the CEFIC composition stipulated by art. 13 of Decree No. 10.900/2021 relies exclusively on members of the federal government: representatives of the General Secretariat of the Presidency, the Ministry of Justice and Public Security, and the Ministry for the Economy.

Note that the CEFIC was created only recently: precisely how its relationship with the ICN Management Committee will be constituted is not clear, since initially there appears to be some overlapping policies and structures covered by both entities.

As noted above, the multisectoral composition of committees managing complex public policies is not unusual in Brazilian history because developing and managing this type of public policy requires a plurality of visions for all sectors of society to be benefited. By prioritizing a non-multisectoral composition of bodies such as CGICN and CEFIC, the active involvement of some sectors of society may be compromised, particularly those that will benefit and be directly affected by choices related to the organization of the ICN, and the gov.br platform.

12 Per Art. 2 of Decree 10.900/2021, "the Citizen Identification Service comprises procedures for managing and verifying the identity of natural persons before the direct federal, autarchic and foundational public administration by means of the gov.br platform."

3.2. ICN's information architecture: centralized structure option

The National Civil Identification Law establishes an information architecture that addresses the constitution of the ICN Database (BDICN) and determines the flow of its personal data within the public administration.

A reading of article 2 shows that the legislative opted for a centralized information architecture because the ICN Database was constituted by concentrating several databases previously created by the government. Comprising mostly biometric data, initially, per the LICN arrangement, this database would be managed by a single institution of the government: the Superior Electoral Court (TSE).

More specifically, according to the legal provisions, the ICN Database consists of the Electoral Court's biometric database - administered by the Superior Electoral Court - the National Civil Registry's Information System (SIRC) - which gathers data related to births, marriages, deaths and stillbirths produced by civil registry offices for natural persons - and the National Civil Registry Information Center (CRC Nacional) - the latter controlled by the National Council of Justice - as well as other data not available in the SIRC, but which are found in other databases managed by the Electoral Court, the identification institutes of the state governments and the Federal District or the National Institute of Identification, or data made available by other bodies, respecting later definitions of the ICN Management Committee. The flowchart below shows the composition of the BDICN:

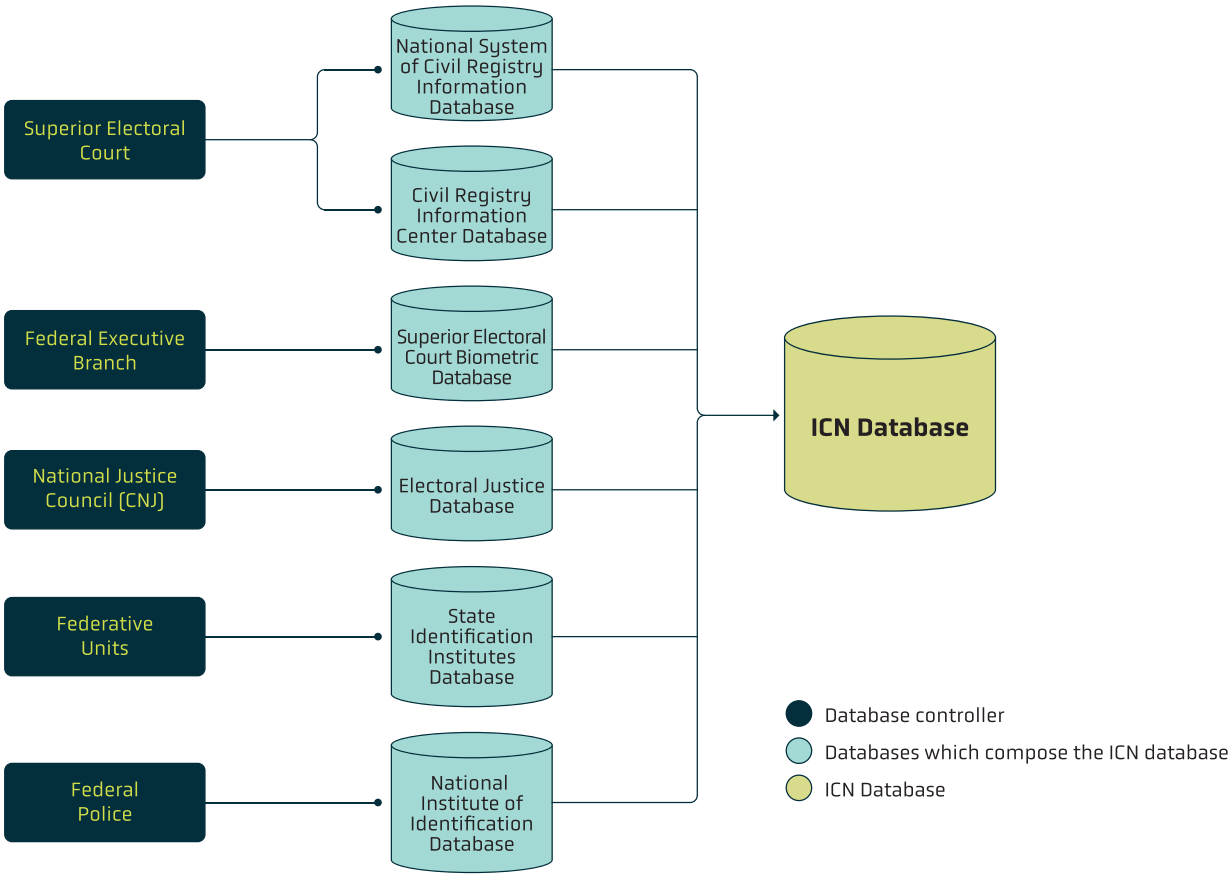


Figure 1
ICN's Information architecture.

The LICN authorizes access to the BDICN for both the Executive and the Legislative Powers at all federal, state, and municipal levels. The only exceptions made are for access to electoral data, which the Electoral Court alone may access. Law 13.444/2017 also enables the Superior Electoral Court to offer citizen authentication services to private sector entities by using biometric data from the ICN Database.

Although the ICN Law establishes a centralized information architecture, this way of structuring a single national civil identification system is not exactly a novelty, since, as discussed in Chapter 2 hereof, the same option was made when the constitution of the RIC was negotiated. On this point, however, it is important to mention that there are alternatives to the centralized architectural model for digital civil identity that have been implemented - or actors have attempted to implement - in Brazil.

As noted in section 2.1, the RIC's implementation was preceded by a wide-ranging exploratory study of the best ways of structuring a unique identity system for Brazil. These studies were conducted by the Ministry of Justice and Universidade de Brasília, based on

a Technical Cooperation Agreement that resulted in several technical reports. Prominent among the documents produced is the technical report on "Research Characteristics and Questions on Identity Management", published in 2015, which posits four models for Electronic Identity Management Systems (locally SGIds): centralized, traditional, federated, and user centered.

Before going into details of these models, some definitions of components that constitute an SGId must be noted. An electronic identity management system is "characterized by the following elements: **user** - actor wishing to access a resource; **identity** - set of user attributes; **identity provider** (IdP) - person/entity in charge of managing identities of its users and authenticating them; **service provider** (SP) - offers resources to authorized users after verifying the authenticity of their identity and after proving that the latter holds all attributes necessary for access" (BHARGAV-SPANTZEL *et al.*, 2007, apud UNIVERSIDADE DE BRASÍLIA, 2015, pp. 13-14)

The model referred to as the "centralized citizen identification system"[13] shows one single identity provider, which will oversee the authentication of users and the provision of services involving data concerning them. In this structural arrangement, the identity provider enables service providers to share user identities between them, allowing the use of a single or unique identity (UNIVERSIDADE DE BRASÍLIA, 2015). This model is criticized precisely because the identity provider has power over users' data, which does not guarantee that their personal information will not be shared with third parties in an abusive manner (UNIVERSIDADE DE BRASÍLIA, 2015).

On the adoption of centralized models, Kenya's "Huduma Namba" digital identity system was brought before the High Court of Kenya and several experts were heard, in particular the submission from expert witness Anand Venkatanarayanan, who noted that centralized information architectures for digital identity are more likely to be targets of security incidents and are therefore more vulnerable architectures from a data security point of view. He added that the option for centralized systems is not in line with modern developments in information architectures, which point toward decentralized systems as the model to be followed (REPUBLIC OF KENYA, 2020).

As alternatives to the centralized model, there are the traditional, federated, and user-centered models. Per Wangham *et al* (2010), the traditional model is widely used in online computer systems. Users are identified separately by each service provider, which also acts as an identity provider. Therefore, users must create a credential for each service

13 Some countries, including Kenya, Nigeria, India, Peru and Argentina, have opted for centralized identity systems.

provider with whom they wish to interact, so there is no data sharing between the various service providers (WANGHAM *et al*, 2010).

The federated identity model, then, relies on user authentication distributed across different identity providers located in different administrative domains, e.g. a company or a university. Wangham *et al* (2010) state that administrative domains consist of multiple service providers, users, and one single identity provider. By allowing identities issued in each administrative domain to be recognized and therefore authenticated by another domain, the federated model helps manage user identities, so that they do not have to deal with multiple identities and be repeatedly subjected to the authentication process (WANGHAM *et al*, 2010).

Finally, the purpose of a user-centered model is to give users control over their digital identities (UNIVERSIDADE DE BRASÍLIA, 2015). In this model, the user's identities are stored on their own physical device, allowing them to choose which of the identity providers will use their data, regardless of the service providers that wish to use them, and without having to submit their personal data to these service providers (UNIVERSIDADE DE BRASÍLIA, 2015). In this model, identity providers continue to act as a trusted third party in the interaction between users and service providers, but they are guided by the interests of users rather than the interests of service providers (UNIVERSIDADE DE BRASÍLIA, 2015).

Below, figure 2 (WANGHAM *et al*, 2010), schematically shows how traditional, federated, centralized, and user-centered electronic identity management models work:

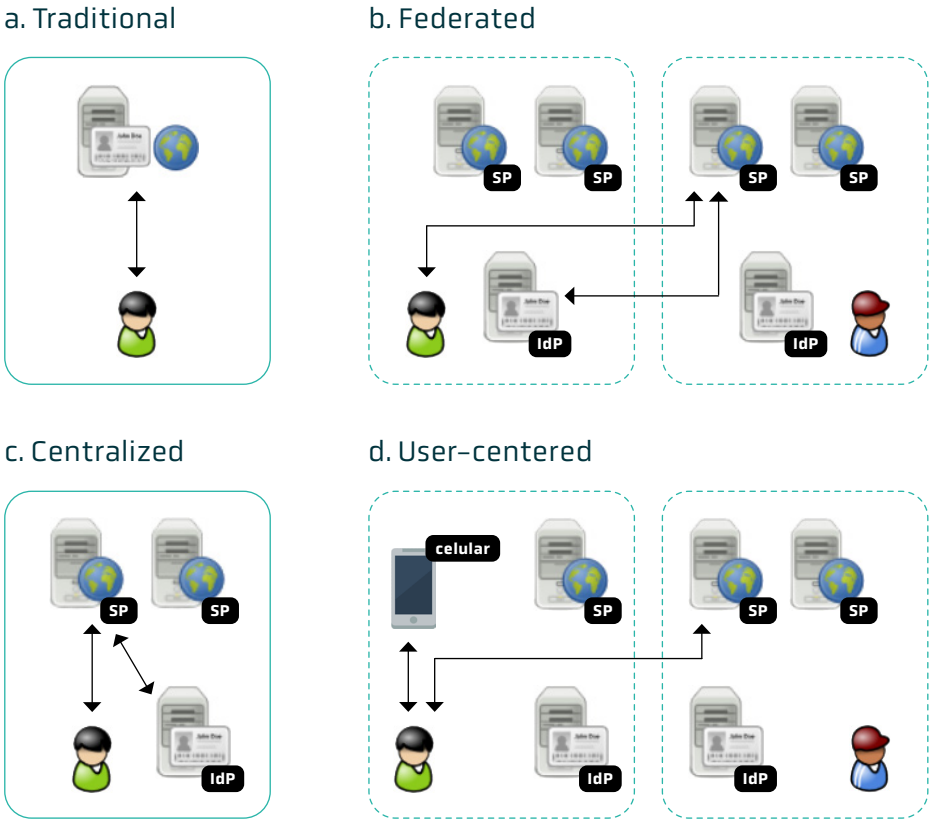


Figure 2
Identity management model classification.

When discussions around the National Civil Identification Draft Law started in 2015, studies related to the RIC were halted. Although the reports produced show the existence of different Electronic Identity Management System models, the Brazilian State opted for the centralized model, and this option was consolidated when the LICN was promulgated. Apparently, this process took place without broad public debate or any methodologically grounded systematic assessment of costs and benefits incurred by implementing each of the abovementioned models.

3.3. Legal discipline of personal data protection and use of BDICN to authenticate citizens on gov.br

After briefly explaining how the ICN's information architecture is structured and how its database is built, this section looks at potential conflicts between the LGPD and the use of the BDICN to authenticate citizens on gov.br. These conflicts arise from the processes of structuring both the BDICN and gov.br.

a. Data security and State Surveillance

As shown above, Brazil opted for a centralized identity system whose database - the ICN Database - originated from merging several other databases. One of the main risks that arise from this option involves data security, insofar as a single security incident may cause exposure or undue access to a large quantity and wide range of personal data, including sensitive data. In this respect, note that Argentina's centralized civil digital identity system was affected by a security incident in 2021. On that occasion, the group that organized the attack on the system posted photos of identity documents on social networks, so documents could be issued for these people, as well as the number internally used by the government and assigned to each citizen (BRODERSEN; BLANCO, 2021) and (BRODERSEN; BLANCO, 2021b).

Similarly, in 2018, the database of the Indian identity system, Aadhaar, also centrally organized, was investigated after an unauthorized access event. Reporters from Tribune (newspaper) were able to buy a username and password to access the web site of the civil identity database (UIDAI), which allowed them to look up any Aadhaar number on the web site and access the photograph, name, address, phone and e-mail of the citizen whose Aadhaar number they had searched (BBC, 2018).

Returning to Brazil, an important point to note is that the last few years have seen a series of significant security incidents involving public databases, such as those of the Ministry of Health and the Ministry of Education, in 2020 and 2021 respectively (IDEC, 2020) and (NAÍSA, 2021). Moreover, in December 2021, over a week, the same group of hackers invaded servers managed by the Ministry of Health, Ministry for the Economy, National Transport Agency and Digital Government pages (MURAKAWA, 2021).

Unsurprisingly, data security is a latent concern for the LGPD, and its art. 49 states that any system used to process personal data must be structured to meet security requirements. The Law's art. 47 also highlights the obligation of processing agents - or any other person intervening in one of the processing stages - to ensure data security in relation to personal data, even when processing has ended. The LGPD's art. 46 also mentions security, technical and administrative measures taken to protect personal data from unauthorized access and accidental or unlawful situations in which data are destroyed, lost, altered, communicated or any form of inappropriate or illicit processing.

The LGPD clearly states that data security considerations must be incorporated into the architecture of any system as of its structuring. Building a centralized system like the ICN involves more security risk, which must be - also to a greater extent - addressed.

The existence of centralized systems for processing personal data does not seem to be the LGPD's legislative preference for data processing undertaken by the public authorities. The LGPD's art. 25 stipulates that data must be kept in an interoperable and structured format for shared use, thus foreseeing a need to share (exchange) data between different public authorities and entities to execute public policies.

The option for a centralized model necessarily corresponds to a higher-level governance complexity. As a rule, this is a model that may not exactly discourage basic good practices but does at least make them more challenging, such as minimizing data collection, data life cycle, identity management, and preventing security incidents. On this subject, Lister (1970) states that there are growing opportunities for governments to monitor their citizens and broaden or deepen any surveillance initiatives due to the existence of large-scale centralized personal data systems, which may cause fundamental changes in society and the balance of power between state and citizen. More specifically, the author lists six immediate privacy threats arising from these systems (LISTER, 1970, p.209):

(1) As data storage and search systems become more efficient, there is no incentive to restrict data collection to the essential, so more data are collected than actually needed, either immediately or prospectively;

(2) More efficient storage means there is no incentive to discard data, which may be more easily retained, even if it is also more easily deleted;

(3) New data systems may use data more thoroughly: data may be correlated to reveal patterns of beliefs or behaviors. This means that a large database may be accurately searched, even for a relatively low priority purpose;

(4) Content may be disseminated more easily: information that was previously only available locally will be accessible to anyone in the country that has access to a terminal;

(5) The mere fact that data is given by a system may make it seem more reliable or valuable to its recipient, which may lead to the loss of critical ability to assess the possibility of the information being wrong or the need to verify, since the data may become obsolete;

(6) The damage that these large centralized systems cause in cases of error is compounded. Conversely, if data circulates only in a limited community, the damage in the event of a mistake would be similarly limited.

In a nutshell, the concentration of data, as in the ICN Database, necessarily implies higher levels of risk exposure and citizen vulnerability. Lyon (2009:4) explains this point: confronting these systems, a citizen becomes observable across their different roles - as consumer, worker, retiree, traveler, (potential) criminal, etc. By condensing all these social spheres, an information flow is more likely to be abusive (NISSENBAUM, 2010).

b. Cases of personal data processing by the Public Authorities

As outlined above, among the data gathered in the ICN Database there is, in addition to a series of non-sensitive personal data, an important volume of sensitive data, as defined in the LGPD's art. 5, item II: biometric data from electoral court systems and race and ethnicity data from the National Civil Registry Information System (SIRC) and the National Civil Registry Information Center (National CRC).

Any personal data processing activity must be based on one of the legal grounds stipulated in the LGPD's art. 7 or, in the case of sensitive data, it's art. 11. When a government processes data, these provisions must be interpreted in conjunction with the same law's art. 23, which states that personal data processing by this type of agent must necessarily serve a public purpose.

The constitution of the ICN Database and its use to identify citizens in transactions involving public and private entities is directly based on the ICN Law, which attributes to the Electoral Court (TSE) competence to manage all citizens' personal data, both sensitive and non-sensitive. In this respect, justifying data processing activities related to maintenance of the BDICN in terms of the LGPD's art. 11, item II, which mentions the "controller's legal or regulatory obligation" seems adequate.

From another point of view, when the ICN database is used to authenticate users on gov.br, legal grounds that might be argued by the public authority for personal data processing would be the execution of public policy stipulated in the LGPD's art. 7-III and art. 11-II b. In this case, the public policy in question would be access to public digital services, precisely through the gov.br platform.

On the appropriate option for the legal grounds being the execution of public policies for data processing, the ANPD's guidebook on "Processing Personal Data by the Public Authority", published in January 2022, conceptualizes the term public policy and unfolds it in two respects. The first is the existence of a formal act that institutes the policy (whether of a normative nature, such as law or regulation, or by contractual means, such

as contracts, agreements, and similar instruments). However, the guidebook emphasizes that - for sensitive data processing - there is no reference in the LGPD to public policies established through contractual arrangements. For these activities, a public policy stipulated by law or regulation would be required, since hypothetical cases of sensitive data processing are more strictly disciplined (ANPD, 2022).

Also, according to the ANPD (ANPD, 2022), another relevant aspect of the configuration of a public policy is material: "the definition of a specific governmental program or action to be carried out by a public entity or body." (ANPD, 2022, p. 13). As a rule, therefore, the content of a public policy would include its objectives, goals, final dates, and means of execution (ANPD, 2022).

In the case addressed by this policy paper - the use of the ICN Database to authenticate users on the gov.br platform - there is a Technical Cooperation Agreement, signed on March 15, 2021, by the General Secretariat of the Presidency, Ministry for the Economy and the Superior Electoral Court to: "I – Specify and implement the provision of the BDICN data verification service through the GOV.BR platform." (BRAZIL, 2021b). The public policy in question here is, therefore, disciplined by a contractual arrangement. This draws attention since there is a large volume of sensitive data processed by the public authority to enable the ICN and the use of its database for citizen authentication on gov.br. On this basis, the requirements for proper use of legal grounds per art. 11-II (b) would not be met[14].

c. Centrality of biometric data and large-scale processing

As extensively noted above, the ICN Database consists of biometric data from the Electoral Court's biometric database that are initially collected for the purpose of making the electoral process more secure (TSE, n.d).

An item posted on the Superior Electoral Court (TSE) website, updated May 17, 2022, states there are more than 118 million people, about 80% of the Brazilian electorate, who have their biometric identification registered with the Court (TSE, 2022b). Biometric identification data covering the entire electorate are to be collected by 2026.

Biometrics, one of the techniques used by ICN and the main one used to authenticate users on the gov.br platform, is the set of methods and procedures used for the recogni-

14 The gov.br website is governed by Decree 8936/2016 and the ICN by Law 13444/2017.

tion of individuals based on their physical, behavioral, and physiological attributes, such as their fingerprints, face, iris and voice (DANTCHEVA, ELIA and ROSS, 2016). A classic biometric system on these lines collects biometric data from a given individual, extracts a series of characteristics from them, and compares them to others found in databases to verify that a given subject really is who they say they are (DANTCHEVA, ELIA and ROSS, 2016). Dantcheva, Elia and Ross (2016) add that other types of data subjects' characteristics (such as age, gender, and ethnicity) may be deduced from biometric data.

Since the ICN Database is not only centralized but also contains biometric data, a potential security incident would be more severe[15]. The United Nations High Commissioner for Human Rights Report of August 2018 (UNITED NATIONS, 2018) stated:

> The creation of mass databases of biometric data raises significant human rights concerns. Such data is particularly sensitive, as it is by definition inseparably linked to a particular person and that person's life, and has the potential to be gravely abused. For example, identity theft on the basis of biometrics is extremely difficult to remedy and may seriously affect an individual's rights. Moreover, biometric data may be used for different purposes from those for which it was collected, including the unlawful tracking and monitoring of individuals. Given those risks, particular attention should be paid to questions of necessity and proportionality in the collection of biometric data. Against that background, it is worrisome that some States are embarking on vast biometric data-based projects without having adequate legal and procedural safeguards in place. (UNITED NATIONS, 2018, p.5).

Although the LGPD does not provide a definition of biometric data, its art. 5-II classifies them as sensitive personal data. For this reason, they are assigned a differentiated and more protective regime, as it is understood that processing this type of data has

15 "Conceptualizing biometric data is difficult. But, in a tight synthesis, breaking down the word in question, it could be said that they are data that measure the body characteristics of a particular individual. Therefore, such data represent a unique particularity of the individual since they cannot be altered or modified because they are "stuck" to the uniqueness of the human body. Therefore, other personal data, such as identity registration and the number in the national register of individuals, may even be considered as unique identifiers, but not with the degree of precision and particularity of the biometric data. This is because biometric data are unalterable as a result of body uniqueness, unlike what occurs when data is attributed to an individual by state control. In this sense, biometric data identify a subject at a global level, unlike the registration of identity that has a national scope. Because of this immutability, singularity and scope is that biometric data should be considered as sensitive data, as they are unique identifiers with the highest degree of precision that no other data has the same capacity. For this reason, biometric data can be as or more harmful than other sensitive personal data. The most diverse fraudulent activities can arise from its access, further enhancing the so-called identity thefts." (GPOPAI, 2015, p.7).

greater discriminatory potential (KONDER, 2019). In this respect, the LGPD's Section II, states that sensitive data may be processed only: (i) with the data subject's specific and distinct consent or that of their legal guardian, for specific purposes; or (ii) without the data subject's consent, as long as it is indispensable for the execution of certain hypotheses exhaustively stipulated in art. 11-II.

Among the legal grounds for processing sensitive data without obtaining a data subject's consent, in relation to the use of the ICN Database to authenticate citizens on gov.br, the LGPD's art. 11-II(b) mentions the possibility of "shared processing of data necessary for the execution, by the public administration, of public policies stipulated in laws or regulations" (BRASIL, 2018). The option to undertake a certain data processing activity based on these legal grounds, however, per General Data Protection Law's art. 11, paragraph 2, evokes the need to publicize the exemption from data subject consent requirements.

In this respect, despite personal data being processed by the public authority to implement the National Civil Identification and citizen authentication services on the gov.br platform being supported by the principle of legality[16], publicizing the exemption from data subject consent requirements in both processes is a fundamental element for the public authority's LGPD compliance.

In the case of the ICN Database being used to authenticate citizens on gov.br, the requirement to publicize details of data processing should be more clearly fulfilled. On these lines, an important aspect is the obligation to post the user agreement and specific privacy policy for user authentication on the gov.br website so that users may refer to it at any time. At the time of writing this report, these documents were only available when creating an account on the website and when logging in to the platform through mobile devices; subsequently, they are not easily accessible[17]. In other words, given the LGPD's provisions, a transparency journey is to be recommended: in addition to notifying data subjects of processing at other times rather than just when entering the system; there should be an interface showing more than just text content, thus quantitatively and qualitatively aggregating information for users.

16 The Principle of Legality can be understood as a "(...) basic guideline for the conduct of Administration agents. It means that any and all administrative activities must be authorized by law. If not, the activity is illegal" (FILHO, 2020, p. 95)

17 From browsing the portal, it is possible to identify the term of use referring to the use of navigation information on gov.br, with no mention of the authentication process for users of the platform. To see more, visit: https://www.gov.br/pt-br/termos-de-uso.

Still concerning the use of biometric data by the National Civil Identification and for the authentication of citizens to access public services through gov.br, a relevant issue concerns the quality of data, established in the General Personal Data Protection Law's art. 6-V, as one of the principles that should guide all personal data processing activities. The legal provision states that the principle of data quality is characterized by data subjects being assured that data are accurate, clear, relevant, and updated, to ensure the data processing purpose is fulfilled (BRASIL, 2018).

This is a Brazilian version of the principle of accuracy set forth in the Council of Europe's Convention 108 and the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, published by the Organization for Economic Cooperation and Development (OECD). The data-quality principle, according to Danilo Doneda (2019), involves assuring data subjects that their stored data correspond to reality and are faithful to it, based on the notion of personal data being processed carefully and correctly and being updated as and when needed (DONEDA, 2019, p. 182). In short, like other personal data protection principles, data quality should guide any personal data processing activity in order to avoid discrepancies related to the data used.

Based on this concept and turning to the ICN and gov.br, the Superior Electoral Court stated that some inconsistencies had been identified in the ICN Database, specifically in its biometric database. In 2018, according to the electoral entity, some 9 million voters – corresponding to 12.21% of those who voted in that year – had problems with immediate biometric identification at the time of voting (PUPO, 2018). The Court stated that this number was equivalent to those of voters who had not used biometrics because the identification process could not be concluded, and voters who were only able to be biometrically identified after several failed attempts.

On the same lines but more recently in August 2021, the TSE set up a commission to manage biometric discrepancies found in the Electoral Registry (TSE, 2021c), named The Management Committee of the Process for the Treatment of Electoral Registry Biometric Duplicates or Multiplicities, to correct these discrepancies. Since 2014, there have been a total of about 52,000 cases related to biometric duplicities or pluralities.

Despite efforts to ensure data quality, the more than 50,000 cases of discrepancies detected by the Electoral Court show the need to adhere to the data quality principle, all the more because the Electoral Court has been taking steps towards a larger biometric database, for example, the National Civil Identification Action for Prisoners (TSE, 2021d) undertaken by the National Council of Justice (CNJ) and the TSE.

Carefully upholding the principle of data quality is essential, insofar as any violation would entail the risk of excluding data subjects from access to the gov.br platform's public services and to public policy for civil identification. They would be segregated because correct user identification and authentication becomes difficult and/or unfeasible if inaccurate biometric data have been collected.

d. Secondary use and shared use of personal data in the context of public authorities

The elastic notion of compatibility for secondary uses of personal data

Conceptually, the secondary use of personal data is characterized when it is processed for a purpose other than the one that justified its collection (WIMMER, 2021a). In the case analyzed in this report, an important aspect to be considered is the existence of two separate points in time to assess two distinct layers of secondary uses of data, in general referring to the BDICN: (i) when building the ICN Database; and (ii) when using the ICN Database to authenticate citizens on gov.br.

As shown above, the ICN Database is regulated by law (Law 13.444/2017, art. 2) and is built from other databases, in other words, by merging previously existing databases. The BDICN data were initially collected for specific purposes by each of the original databases that were subsequently merged- for example, the Electoral Court's biometric data were collected for the purpose of voting in elections while civil registration data were kept precisely for civil registration purposes. When they are added to one single database, i.e. the BDICN, these personal data are for secondary use.

In addition to the National Civil Identification, this report focuses on the use of this database to authenticate citizens accessing public services through the gov.br platform. To do so, there is a second stage in which the secondary use of data is verified. The BDICN was built for the purpose of supporting National Civil Identification policy per the LICN's art. 1, whereas their data are being used for another purpose in this case - namely to authenticate citizens accessing public services through gov.br.

An important aspect to note is that the LGPD does not forbid processing data for secondary purposes. On the contrary, it expressly allows this but requires the operation to verify compatibility between the secondary use context and the context in which the data was originally collected. The LGPD mentions "compatibility" in three instances, two of them

in the passages that prescribe the concept of the principles of purpose and adequacy[18]. There is a complementary relationship between them due less to their sequential topographical allocation and more to the grammatical structure of said provisions, as in so-called principal and subordinate clauses. While the principle of purpose introduces the idea that "subsequent processing" must be compatible, the adequacy principle explains that adequacy may be gauged "depending on the context" of the data processing, as the following conceptualization and schematization show[19]:

> I - purpose: processing done for legitimate, specific and explicit purposes of which the data subject is informed, **with no possibility of subsequent processing that is incompatible with these purposes**;
>
> II - adequacy: **compatibility of the processing** with the purposes communicated to the data subject, **in accordance with the context of the processing**[20];

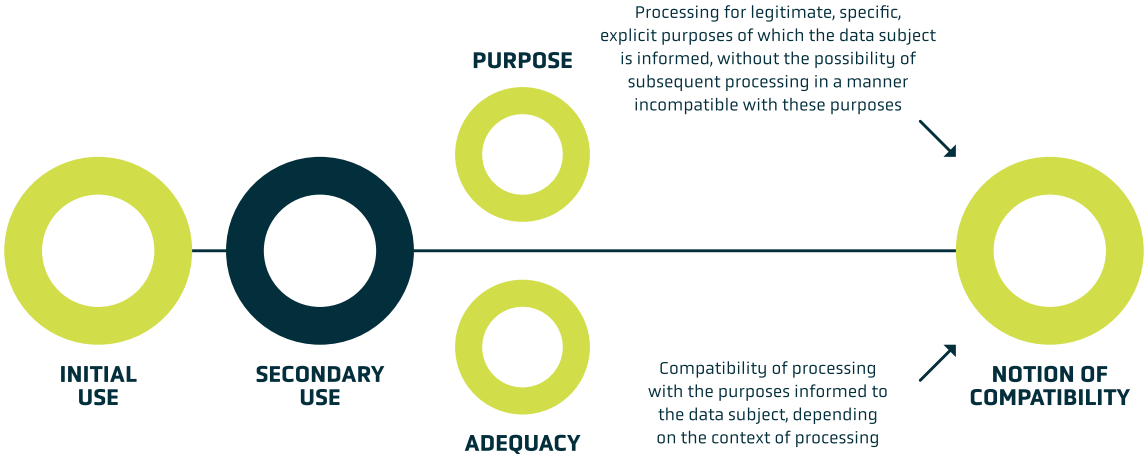


Figure 3
Schematization of personal data secondary use.

By connecting these two principles with the bona fide (good faith) principle and contextual privacy theory (NISSENBAUM, 2010), Bioni (2021) notes how this method focuses on the extent to which an information flow is, and should be, dynamic. In addition to the LGPD's text being close to a theory that eschews any static definition of compatible data

18 The third directly relates to the legal basis of consent (Art. 9, paragraph 2).

19 Data Privacy Brasil Ensino (educational institution) authorized use of this image from the first class of its course on "Personal Data Privacy and Protection: theory and practice".

20 TN2: Translation of LGPD quoted from: https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/

processing, lawmakers made use of an indeterminate legal concept - a legislative technique that crafts legal imperatives abstractly to the point of requiring their interpreter to undertake a meta-legal search of the characteristics of the context of the relationship between the data subject and the processing agent:

> not delimited by a specifically rigid goal - in line with the 'certain purposes' expression (...) but directed to a range of actions that may be executed in the context of a relationship. By doing so, contextual privacy proves itself to be useful, , since it is sufficiently elastic to govern the secondary use of personal data that cannot be previously specified and strictly controlled (...) a more open-ended analysis that inquires in relation to the two characteristics, if (...) they are in accordance with the context of the relationship underlying the information flow (...) This is the element that affords a minimum of predictability (security) in relation to the information flow's spaces of uncertainty. (Bioni, 2022, p. 231-234)

Aware of the need to clarify this legal concept of "compatibility", the ANPD (2022) suggests considering the following aspects:

> (i) the relevant context and circumstances of the specific case; (ii) the existence of a factual or legal connection between the original purpose and the one on which the subsequent processing is based ; (iii) the nature of the personal data, taking a more cautious attitude when processing sensitive data ; (iv) data subjects' legitimate expectations and possible impacts of subsequent processing on their rights; and (v) the public interest and specific public purpose of subsequent processing, as well as its link with the legal powers of the bodies or entities involved, per the LGPD's art. 23 (ANPD, 2022, p. 13)

On the data subject's legitimate expectation, opinion 06/2014 of WP 29 on Legitimate Interest states that the considerations for assessing data subjects' legitimate expectations concerning the secondary use of data collected are similar to the purpose principle:

> (...) It is 'important to consider whether the status of the data controller, the nature of the relationship or the service provided, or the applicable legal or contractual obligations (or other promises made at the time of collection) could give rise to reasonable expec-

> tations of stricter confidentiality and stricter limitations on further use. In general, the more specific and restrictive the context of collection, the more limitations there are likely to be on use. Here again, it is necessary to take account of the factual context rather than simply rely on text in small print. (WP 29, 2014, p. 40)

Considering the information given, in order to assess the secondary use of data for the Brazilian policy on digital civil identity and platformed public services, first, one should analyze the databases comprising the ICN and the secondary use when they are operationalized for a unified ICN base. Secondly, it is also necessary to assess the secondary use of the ICN Database itself when accessing gov.br. This is the context and circumstances in which the activities take place.

Moving on to the following requirements established by the ANPD for the assessment of the secondary use of data, it appears that, in general, there is a legal connection between the original processing purpose and the purpose of the secondary use – be it through LICN or through the Technical Cooperation Agreement signed in March 2021 for the use of BDICN in gov.br. In relation to the first processing layer, i.e. building the ICN Database, the legal connection between the processing's original and subsequent purposes is established by the LICN's art. 2 stating which databases the ICN will use. In relation to the second processing layer, the time when the ICN Database is used to identify a citizen in gov.br, section 1.2 of the Technical Cooperation Agreement signed by TSE and SGD determines BDICN data verification services through the gov.br platform. (BRASIL, 2021b).

In parallel, all the databases comprising the BDICN are known to contain sensitive data, mostly used for the purpose of identifying citizens. This is clearly shown by analyzing which data are collected by processing agents, such as: the Electoral Court, which collects voters' fingerprints and photos; civil registry offices that reveal race/ethnicity data, when issuing death certificates per Law 6.015/1973 art. 80, paragraph 3; and the identification institutes that collect right-hand thumbprints and photograph the identified person per Law 7.116/1983 art. 3 (f), in order to issue identity cards. Sensitive data are, of course, processed in a more protective regime, so their secondary use must also require greater caution.

Furthermore, as noted above, a data subject's legitimate expectation is also an element that may be considered when analyzing the secondary use of data (WP, 2014). In the cases analyzed here, when considering the context in which data were collected to build the databases comprising the ICN, there was clearly an expectation of restricted use of the data. This means that the secondary use of data - identified both for building the

BDICN and using of this database to authenticate gov.br platform users - may impact data subjects' rights by subverting their legitimate expectations.

Finally, regarding the public interest and purpose requirements for operations, there is clear fulfillment. After all, even though they pose major risks to be addressed, unified civil identification and digitized public services policies are backed by an attempt to diminish sub-registries and broaden Brazilians' access to services.

Despite the importance of the ANPD establishing general compatibility criteria, it is necessary, depending on the specific case involved, the definition of new parameters for an investigation of this nature may ensure a more granular and attentive analysis of the situation. In this respect, two new criteria have been posed to scrutinize the compatibility of primary and secondary uses of data per ICN and gov.br policies to discuss the issues in more depth: the nature of the data processing agent and the level of connection between the information architecture of the database primary and secondary use of data.

Considering these new criteria, added to the above thoughts, made from the parameters suggested by the ANPD, the conclusion reached was that the level of compatibility between the purposes established for the initial and secondary use of these same data was medium for the first stage of secondary data use - i.e. in the composition of the BDICN, considering most of the original databases merged to create this large database - detailed one by one below. This conclusion, however, excludes the use of the Electoral Courts' biometric database to create the BDICN insofar as, in this specific case, no factual connection was identified between the original purpose that justified collecting biometric data and the purpose established for secondary processing, which resulted in a low level of compatibility.

In relation to the Electoral Court's biometric database, a voter's fingerprint, signature, and photo are collected for a very clearly delimited purpose: identifying the citizen as a voter. In the ICN's subsequent processing, the data subject's individualization is directed towards a much broader range of transactions, which potentially spreads throughout all relations between citizen and State, and even with private entities (JUSTIÇA ELECTORAL, n.d). Although they are linked by the same macro perspective, which is the citizen's individualization, there is a significant distance between the initial collection's context - the citizen in their role as a voter before the TSE (Judiciary) as the controller - and the aforementioned secondary uses - the citizen in their condition of potential assisted by the State before the Executive Power as the controller – also as a potential consumer when private entities are brought into the chain. As a result, there is a transgression of the information flow between very different spheres capable of thwarting

the data subject's legitimate expectations. All of this, added to the high-level criticality of biometric data - even compared to other types of sensitive data (see chapter 3, section 3.3 c), leads to an assessment of a low level of compatibility between the original purpose and secondary use of the Electoral Court's biometric data to build the BDICN.

In turn, the SIRC and National CRC databases, which were also merged to build the BDICN, have been built by merging civil registry office databases in which birth, marriage, death, and stillbirth events are recorded per Law No. 6.015/1973. Like the ICN, they too bear witness to a natural person's biographical attributes, including sensitive data such as race and ethnicity-related aspects, without which a series of rights could not be exercised. Moreover, they also serve the purpose of identifying a citizen in their relations with the State. So there is a factual legal connection between the original purpose of collecting the citizen's civil life registration data for the ICN's secondary purpose.

However, there is a structural difference between the notarial office system and the ICN from the information architecture point of view. While civil registry offices are structured following a decentralized rationale, the ICN is a centralized model, one that aggregates data from several other spheres. In addition, collecting data from their context in the notary system, poses an expectation of restricted use such as obtaining a birth, marriage, or death certificate. This is quite remote from the secondary purpose of building the ICN database, which makes data available to a wide range of government entities, all citizen-government relationships, and even private individuals. So, there is clearly a low level of compatibility between the information architectures of the ICN and the CRC, so ultimately there would be a medium level of compatibility between primary and secondary data uses in this case.

Finally, the databases of the Identification Institutes managed by State governments, the Federal District, and the National Identification Institute, which also comprise the ICN, contain data from identity cards issued by these entities per Law No. 7.116/1983. Like the ICN and civil registry offices, the bases of the Identification Institutes of the States and Federal District and the National Institute of Identification attest to the natural person's biographical attributes required to exercise a series of rights. So, there is a factual connection between the original purpose of collecting data, recording data from a citizen's civil life and the ICN's secondary purpose of identifying citizens in their relations with government and private entities.

In parallel, similarly to the databases of the SIRC and the National CRC, the databases of the Identification Institutes of the States and the Federal District and of the National Institute of Identification record biographical data of the natural person necessary for

the exercise of a series of rights, although from opposite architectures: decentralized in the identification institutes and centralized in the ICN. There is also a legal connection between the purposes established by the LICN of identifying the citizen in their relations with the State and individuals and the purpose established in the identity card law (Law nº 7.116/1983, art. 6) included in the identity card for relationships with third parties. There are sensitive data involved in the operation, since, according to Law nº 7.116/1983, art. 3, paragraph (f), the identity card contains a photograph and the fingerprint of the right finger of the identified person, which are, depending on the context in which they are processed, biometric data. As for the legitimate expectations of the data subjects, there is the expectation of restricted use of these data, due to the context of the collection, whose specific purpose was to obtain a document - in this case, the RG. From the weighting of these criteria, it is understood that, in the end, the degree of compatibility between the primary use of the database of identification institutes and its secondary use in the composition of the BDICN is medium.

Alongside all these activities that involve the secondary use of data in the constitution of the BDICN, there is also the second major stage in which this type of operation takes place: the use of the ICN Database to identify citizens for the gov.br platform. In this case, there is a strong connection between original and secondary purposes: the ICN´s purpose is to provide identification for citizens in their relations with the State and private entities. Since gov.br is the platform that concentrates the State, it can be said that the identification of the citizen in gov.br is covered by the purpose of the ICN. In other words, to the extent that access to digitalized public services is constituted as a State-citizen relationship, it can be said that there is a convergence of the initial and secondary purposes of data processing. There is also a legal connection between these purposes since the use of BDICN in gov.br is regulated by the ACT signed between the federal government and the TSE.

Here, it is difficult to assess the legitimate expectation of data subjects in relation to the use of BDICN for authentication in gov.br, since the constitution of BDICN does not necessarily follow their legitimate expectations, as explained above. Regarding information architecture, both BDICN and gov.br are centralized architectures - BDICN combines several databases in a centralized way, while gov.br combines several sources of government information, at the federal, state, and municipal levels, in a single portal, centralizing the offer of services and public information. Considering the degree of factual and legal connection between the original purpose and the secondary purpose and the degree of connection of information architecture, both high, the compatibility between the original purpose of BDICN and the secondary purpose of its use in gov.br is equally, high.

Regardless of the degrees of compatibility evaluated, it is important to emphasize that the prevalence of sensitive data, which can be seen in all databases, as well as the legitimate expectation of users of more restricted use of data from the context of the collection, recommends greater caution in all the operations of secondary use of the data.

Considering the aspects suggested by the ANPD (2022, p. 13)[21] and the new criteria proposed here, seeking to summarize the above-detailed analysis, the table below was prepared to outline the compatibility between the purpose of the original use and that of secondary uses of citizens' personal data:

21 (i) the relevant context and circumstances of the specific case; (ii) the existence of a factual or legal connection between the original purpose and that on which the subsequent processing is based; (iii) the nature of personal data, adopting a position of greater caution when sensitive data is covered; (iv) the legitimate expectations of the holders and the possible impacts of further processing on their rights; and (v) the public interest and the specific public purpose of the further processing, as well as its link with the legal competences of the bodies or entities involved, pursuant to art. 23 of the LGPD (ANPD, 2022, p. 13)

Database	Data Processing Agent	Notes on data processing agent	Degree of factual and legal connection between original and subsequent purpose	Nature, type of personal data, and Impact on fundamental rights and freedoms	Information architecture – level of connection	Level of compatibility
Electoral Courts' biometric database	Superior Electoral Court	Public Law Legal Entity pertaining to the Judiciary	**Low** (data subject's identification in their specific condition as voter)	**Sensitive** (biometric) and **high impact** due to irreversibility of identity theft	**Low** (does not involve combining other databases)	**Low**
National Civil Registry Information System (SIRC) (Decree 9.929 of July 22, 2019)	Civil Registry Office	Private Law Legal Entity and service by public delegation	**High** (data subject's identification for the exercise of a series of rights involving public and private entities)	**Sensitive** (race and ethnicity) and **high impact** due to irreversibility of identity theft	**Low** (involves database combination, but from a decentralized model)	**Medium**
National Civil Registry Information Center (National CRC) The CNJ's Provision No. 46 (CNJ, 2015)	Civil Registry Office	Private Law Legal Entity and service by public delegation	**High** (data subject's identification for the exercise of a series of rights involving public and private entities)	**Sensitive**[22] (race and ethnicity) and **high impact** due to irreversibility of identity theft	**Low** (involves database combination, but from a decentralized model)	**Medium**
Databases - Identification Institutes of States and DF	Identification Institutes of States and DF	Public Law Legal Entity	**High** (data subject's identification for the exercise of a series of rights involving public and private entities)	**Sensitive** (photo and biometrics) and **high impact** since identity theft is irreversible[23]	**Low** (involves database combination, but from a decentralized model)	**Medium**
National Institute of Identification	National Institute of Identification	Public Law Legal Entity	**High** (data subject's identification for the exercise of a series of rights involving public and private entities)	**Sensível** (photo and biometrics) and **high impact** due to irreversibility of identity theft[24]	**Low** (involves database combination, but from a decentralized model)	**Medium**
BDICN	Superior Electoral Court (controller) SERPRO (operator)[25]	Public Law Legal Entity and Public Company respectively	**High** (data subject's identification for the exercise of a series of rights involving public and private entities)	**Sensitive** (biometric) and **high impact** due to irreversibility of identity theft	**High** (involves combining several databases in a centralized way)	**High**

22 Death certificates contain race/ethnicity information, per art. 80, § 3º, Law 6.015/1973.

23 Identity cards contain fingerprints of the right thumb and 3x4 photographs, per art.3 (f) of Law 7.116/1983.

24 Identity cards contain fingerprints of the identified person's right thumb and a 3x4 photograph per art.3, f, Law 7.116/1983.

25 Contract signed by TSE and SERPRO to "Operate National Civil Identification (ICN) for biographical and biometric verification services, biographical research and issuing National Identification Documents (DNIs)": TSE (2021e).

Shared use of data by public authorities

The LGPD's art. 5 XVI defines shared use of data as:

> XVI – shared use of data: communication, dissemination, international transfer, interconnection of personal data or shared processing of banks of personal data by public agencies and entities, in compliance with their legal capabilities, or between these and private entities, reciprocally, with specific authorization, for one or more types of processing allowed by these public entities, or among private entities[26];

As noted above, the National Civil Identification Law's art. 3 poses hypothetical cases of shared use of data by facilitating ICN database access for the Executive and Legislative powers of Municipalities, States, Federal District, and Federative Authorities, if the data are used for the same purpose as the ICN itself - namely to "identify Brazilians in their relations with society and with governmental and private bodies and entities", per the LICN's art. 1. In addition, there is shared use of data when BDICN enables citizens' authentication on gov.br.

In addition to the LGPD's art. 5, its art. 25, part of the section that governs the public authorities' data processing, stipulates data shall be retained "in an interoperable format and structured for shared use". Further on, the LGPD's art. 26 determines that the shared use "shall fulfill the specific purposes of execution of public policies and legal attributions by agencies and public entities, subject to the principles of personal data protection listed in Art. 6 of this Law.[27]"

In consonance with the legal provisions, ANPD (2022) defined personal data sharing as "processing through which public bodies and entities grant permission to access or transfer a personal database to another public entity or to private entities in order to serve a public purpose" (ANPD, 2022, p.17).

On these lines, the Authority (2022) established the following requirements as principles to be observed by the public authorities for personal data sharing processes: (a) formal-

26 TN3: Translation of LGPD quoted from: https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/.

27 TN4: Translation of LGPD quoted from: https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/.

ization and registration of shared use of personal data by the public authority ; (b) indication of the data shared and the specific purpose of the sharing process; (c) legal grounds (the LGPD's article 7 or 11); (d) processing duration ; (e) transparency and data subjects' rights; (f) prevention and security (ANPD, 2022, p. 17-19). There may be more requirements depending on the particularities of each case: there may be authorization or prohibition for further sharing or subsequent personal data transfer, specific requirements for sharing personal data with private entities as per LGPD, and the drafting of a data protection impact assessment (ANPD, 2022).

So, if there are operations based on shared and secondary use of personal data, a series of more robust governance measures are required, such as those listed above. In the present document, these governance measures should specifically apply to the shared use of the ICN Database by gov.br to identify citizens. This use is regulated in the Technical Cooperation Agreement signed between the Executive Branch and the Electoral Court dated March 2021 (TSE, 2021b; BRASIL, 2021b).

The agreement formalized the shared use of personal data by the public authorities, stating that the ICN Database will be shared for the purpose of "strengthening of an integrated national citizen identification system (...) in the context of the GOV.BR platform" (BRASIL, 2021b). The legal grounds for processing per the General Data Protection Law are not mentioned. As to data processing duration, the agreement poses 60 months that may be extended by the parties for an indefinite number of times. In addition, the document does not mention data subjects' rights or transparency measures for this agreement, or prevention and security measures for personal data processing.

The General Data Protection Law actually is mentioned only once, in the ACT's section 4, which states that one of the Agreement's goals is establishing rules for services to comply with the General Data Protection Law: "in particular, providing tools to ensure the traceability of access to data and management of consent, as well as stipulating the roles that each of the participants will play per Law No. 13.709/2018, particularly its article 7".

This policy paper discusses both transparency and data subjects' rights (Chapter 3, section 3.3f) and aspects of prevention and security (Chapter 3, section 3.3a) within the framework of the ICN. The main conclusions are the ICN's opacity and the difficulty of exercising data subjects' rights as well as the higher level of data security risk due to the ICN's centralized model.

Checks and balances for secondary and shared use of data by the public authorities: information separation theory

Wimmer (2021a) points out as a central problem of the LGPD the existence of a gap regarding the possibilities and limits for the sharing and secondary use of personal data within the scope of public authorities, that is, the lack of clear criteria that discipline such activities. This lack of express limits, in turn, can lead to abusive uses of data, which violate the rights of its data subjects. In view of this situation, the author proposes in her work three parameters to be considered to legitimize the sharing and secondary use of data between public authorities.

The first of them would be the compatibility of purposes between the original treatment and the secondary use, an understanding expressly adopted by the LGPD, as already seen in this report. If there was no such compatibility, two other additional elements, depending on the specific conditions of the case, could be considered to overcome such incompatibility: a new authorization provided by the data subject or the existence of a specific legal provision. Such flexible understandings are supported by the Council of Europe Resolution on the protection of the privacy of individuals in relation to electronic databases in the public sector, of 1974, in the OECD Privacy Guidelines updated in 2013, and also in the logic adopted by the GDPR (WIMMER, 2021a, p. 137). In either case, data protection principles must be applied, through the material and procedural safeguards that are necessary for the processing activity, in addition to providing the affected individual with adequate information about the operation and consideration of constitutional principles that protect individual freedom, privacy, and free development of personality.

Wimmer (2021a) focuses the discussion of data sharing in e-government initiatives, such as gov.br, emphasizing that the debate of sharing and secondary use of data between public authorities poses two opposing perspectives: one that defends broad sharing of extensive data across public entities to offer better public services, to ensure more efficiency with less bureaucracy; and another that points to the risks arising from sharing initiatives such as state surveillance.

Far from representing a conflict between public and collective interests (for better public policies) and a private interest focused on the individual (to protect the right to privacy and data protection), Wimmer (2021a) shows how the right to privacy and data protection has a meta-individual dimension and is also related to the public interest.

This matter of public authorities sharing personal data is being discussed in the case. ADPF 695, which is awaiting the STF's judgment at the time of writing the present (May

2022). The suit discusses the sharing of Citizens' driver's license data, originally collected by Brazil's Traffic Department (DENATRAN), by the Federal Data Processing Service (SERPRO) with Brazil's Intelligence Agency (ABIN), on the grounds stated in Decree No. 10.046/2019. This decree regulates governance for data sharing in the federal public administration and institutes the Citizen Database Registry and Central Data Governance Committee. The same decree exempts actors from any need for technical cooperation agreements or similar instruments for data sharing across federal public administration agencies and entities.

On June 24, 2020, Justice Gilmar Mendes (as rapporteur) rejected the ADPF's precautionary measure, which was deemed moot because the Executive Power had already revoked the data-sharing authorization. However, the decision allowed the action to proceed and highlighted the relevance of its object - Decree 10.046/2019, the Citizen Database Registry:

> (...) the legal regime for sharing data between the Public Authorities' entities and institutions is a matter of extreme relevance for the constitutional protection of the constitutional right to privacy (the Federal Constitution's art. 5 -X), an elementary guarantee for any contemporary democratic society (STF, 2021, p. 47).

Gilmar Mendes analyzed this legislative text to conclude that it flouted the logic of the principle of purpose by diminishing (or sometimes eliminating) barriers to the free flow of shared personal data in the public administration, particularly in articles 5 and 11.

Justice Mendes also noted that recognizing the autonomy of the fundamental right to personal data protection will necessarily lead to an awareness of the legal privacy regime as a structural aspect of democratic regimes rather than a value opposed to the public interest, as mere protection of individual rights. Finally, he added that there is no a priori sign of Brazil's legal system "unrestrictedly authorizing the free flow of data sharing between public authorities, even if used for national intelligence activities" (STF, 2021, p. 38-39). Therefore, the State is not a single or unique information unit.

This notion of the State not being a single or unique information unit was introduced several years ago by Simitis (1987), for whom the purpose principle, as one of the four basic elements of any data protection regulation, may be defined as a normative barrier to unregulated multifunctional use of data. On this basis, the organizational division, currently existing in the modern State's 'direct' and 'indirect' public administration (such as the former's ministerial departments or secretariats and the latter's foundations, regu-

latory agencies, and para-statal entities), should be mirrored from the information aspect. Simitis, therefore, poses an information separation of powers concept: determining the possibility of accessing data depends on the specific function of the governmental agency or entity that intends to process the data and its relation to the purpose that prompted the data collection in question - rather than simply the fact of the processing agent being part of the State (Simitis, 1987) and/or a public interest possibly being served by this instance of data processing.

The Brazilian ICN model - which resulted from aggregating a series of databases that permeate the electoral and notarial sphere, and the Executive Power itself, assuring government agencies and entities extensive access to its databases - directly clashes with the information separation of powers theory. This clash is further aggravated by the secondary use of the ICN data on gov.br, a platform that datafies and projects citizens across all their relations with the State, and in some cases their relations with private individuals too.

This section initially posed a definition of the secondary use of personal data, as well as the importance of the principle of purpose to assess the legitimacy of secondary use. Based on criteria from the ANPD (2022), two instances of secondary use of data by public authorities were assessed and analyzed in this document: the use of databases built by the TSE, SIRC, CRC, and Identification Institutes to comprise the BDICN, per the LICN, and the use of the ICN's database to authenticate citizens on gov.br. Our assessment was based on the level of compatibility between the purpose of the use for which data were originally collected and the purpose of their secondary use. The level of compatibility of the two secondary uses analyzed was rated 'medium'. The sole exception was the electoral database, whose secondary use to build the ICN's databases was rated as showing low-level compatibility.

Having considered and assessed the secondary use of data by the public authority, this section examined the shared use of data by public agents, per guidelines established by the ANPD (2022), used as an analytical tool for the assessment. This section also looked at the case of ADPF 695 and the concept of information separation of powers, which on the same lines show that the State cannot be treated as a single or unique information unit with a free flow of data across government agencies and entities.

Considering the grammar of risks involved in personal data protection, to be detailed in Chapter 5, any abusive shared or secondary use of data that fails to consider the purpose for which data were collected, may be seen as a risk for citizens because data initially collected for civil identification purposes could be misused by state intelligence agencies

for their own activities, as in the concrete case litigated in ADPF 695.

Access to ICN database foreseen in LICN and Draft Law No. 3228/2021

The Civil Identification Law's art. 3 assures access to the ICN's database, except electoral information, for the Executive and Legislative authorities at all levels of the federation. Further on, in the same provision's paragraph 1, the law even stipulates that the Executive Powers of the federated entities may add information from the ICN's database to their own databases, except for biometric data[28].

The federal government's Draft Law No. 3228/2021 seeks to change the National Civil Identification Law in order to allow the ICN's database to be replicated across Federal Executive authorities while no longer excepting biometric data and retaining restricted access for electoral information only[29].

Both the LICN and its proposed amendment aim to eliminate barriers preventing the public authorities from accessing citizens' personal data. In principle, neither LICN nor the proposed amendment require data sharing to serve any specifically determinate purpose, thus contradicting the principle of purpose stipulated by the LGPD. An even more worrying prospect is that shared data could become definitive components of databases built by new entities and public authorities. In addition to posing a critical data security problem to the extent of losing control over who, when and for what purposes data are being accessed, the question one must ask is this: why would a federated entity of the Executive that is engaged in local activities have a national identity database, including data from citizens who are not subject to its jurisdiction?
As emphasized above, any sharing and secondary use of data across public authorities must be guided by data protection principles - in the case of ICN and gov.br, particu-

28 Art. 3 The Superior Electoral Court shall allow Executive and Legislative authorities of the Federative Republic, States, Federal District, and Municipalities access to the ICN database free of charge, except for electoral information.

§ 1 The Executive Authority – of the federated entities may add information from the ICN database to its own databases, except for biometric data.

29 Art. 2 .....

§ 1 The ICN's database will be stored and managed by the Superior Electoral Court, which will ensure it is updated and take measures required to ensure its content's integrity, availability, authenticity, and confidentiality as well as interoperability across governmental electronic systems, enabling the Superior Electoral Court to replicate the database in the Federal Executive Branch's IT environments.

Art. 3 .....

§ 1-A Paragraph 1 may apply to biometric data when expressly authorized in the instrument referred to in § 3 of art. 2.

larly by the principles of purpose, adequacy, and necessity. In this respect Draft Law 3228/2021 has embarked on a collision course with these provisions from LGPD, thus exacerbating the risk for data subjects' civil rights and liberties while the ICN's governance issues become even more complex from a data security point of view.

e. Cross-referencing official databases

Public policies such as ICN are directly related to the implementation of the principle of non-discrimination as one of the fundamental objectives of the Republic per the Federal Constitution's art. 3, as reflected in the LGPD, which lists non-discrimination among personal data protection principles (article 6-IX).

Brazil's General Data Protection Law requires personal data processing activities to avoid unlawful and abusive discrimination. When there is personal data processing inside the Public Administration, assuring this principle involves the need for extensive publicity and transparency.

In the case of the National Civil Identification, the LICN's art. 11[30] stipulates the possibility of cross-referencing official databases for compliance with eligibility requirements that a given citizen must meet to obtain social benefits or continue receiving them.

In this respect, access to certain social benefits would be linked to the process of cross-referencing the beneficiary's personal data for compliance with legal requirements for their access. Hence the risk of this data processing activity excluding people. The UN's Special Report on Extreme Poverty and Human Rights, of October 11, 2019 (United Nations, 2019) notes that States are increasingly using digital technologies and data in their social protection and assistance systems, often in ways that harm the most socioeconomically vulnerable. There is a proliferation of neoliberal values that are hostile to social assistance and protection systems being implemented in conjunction with technology while disregarding human rights:

> The digital welfare state is either already a reality or is emerging in many countries across the globe. In these states, systems of social protection and assistance are increasingly driven by digital

30 Wording of art. 11 of Law 13.444/2017: "The public authorities must offer mechanisms that enable information in official databases to be cross-referenced based on the applicant's tax registration number, thus enabling the agency in question to verify eligibility requirements for granting and maintaining social benefits."

> data and technologies that are used to automate, predict, identify, surveil, detect, target and punish. This report acknowledges the irresistible attractions for governments to move in this direction but warns that there is a grave risk of stumbling zombie-like into a digital welfare dystopia. It argues that Big Tech operates in an almost human rights free-zone, and that this is especially problematic when the private sector is taking a leading role in designing, constructing, and even operating significant parts of the digital welfare state. The report recommends that instead of obsessing about fraud, cost savings, sanctions, and market-driven definitions of efficiency, the starting point should be on how welfare budgets could be transformed through technology to ensure a higher standard of living for the vulnerable and disadvantaged. (UNITED NATIONS, 2019, p.1).

Potentially discriminatory results would arise from cross-referencing databases containing data such as race, ethnicity, and gender that are not necessarily pertinent for the purposes of verifying compliance with requirements for access to social benefits. Since there may well be discrimination against citizens, clear data governance parameters are more crucial than ever to regulate data being cross-referenced to assess eligibility for public policies.

Recently, Dutch tax authorities adopted an algorithmic decision-making system to create risk profiles of individuals applying for childcare benefits in order to detect inaccurate and potentially fraudulent applications at an early stage. Nationality was one of the risk factors used by the tax authorities to assess the risk of inaccuracy and/or fraud in the applications submitted. Research showed how the use of individuals' nationality resulted in massive discrimination based on nationality and ethnicity, as well as racial profiling. (AMNESTY INTERNATIONAL, 2021).

On the same note, returning to the Brazilian context, Justice Luís Roberto Barroso's decision in relation to Writ of Mandamus No. 36150, filed by the National Institute of study and research on Education Anísio Teixeira (Instituto Nacional de Estudos e Pesquisas Educacionais Anísio Teixeira, or INEP) against a Federal Court of Accounts (TCU) ruling that determined the sharing of individualized data from the Education Census and Brazil's nationwide university admission exams (locally known as *ENEM*) to audit conditional social benefits for low-income families (*Bolsa Família*) (STF, 2021).

While acknowledging the TCU's constitutional competence to audit and inspect Public Administration entities' accounts, finances, budgets, and assets, Justice Barroso pointed to the importance of the principle of purpose for personal data collection. His decision found data required by the TCU were collected by INEP to fulfill specific purposes covered by the Institute's assurance of secrecy. In this respect, the rapporteur justice states that sharing these data for a purpose other than initially agreed would undermine the principle of purpose and therefore subvert the authorization of persons who had submitted their data.

This case may be compared with the provisions of the LICN's art. 11. By cross-referencing data in the ICN's database - processed specifically for citizen identification purposes - with other data to assess eligibility for social benefits, the public authority could be breaching the principle of non-discrimination since the results can lead to exclusion and the breach of the principle of purpose, both ensured in Brazil's LGPD[31].

f. LICN omissions: exercising data subjects' rights and ensuring publicity–transparency of personal data processing

As noted above, the ICN is a public policy founded on the principle of legality and based on large-scale personal data processing, especially biometric data - i.e. sensitive data. This means that public authorities' processing personal data from the ICN database, such as authenticating citizens to access public services via gov.br, evokes the need for convergence between two large groups of principles: those defined by the Data Protection Law - which should guide all data processing activities - and the constitutional principles governing the Public Administration (WIMMER, 2021b).

There is an alleged conflict between the need for the Public Administration's activities to be transparent and assuring data protection for data subjects (WIMMER, 2021b). However, the issue may be characterized as just an apparent conflict, since the transparency of the public authorities' processing activities are crucial to uphold data subjects' rights, especially since the General Data Protection Law's art. 6 - VI defines transparency as "guarantee to the data subjects of clear, precise and easily accessible information about the carrying out of the processing and the respective processing agents, subject to commercial and industrial secrecy"[32].

31 For shared secondary use of data, see subsection 3.3d of this policy paper.

32 TN5:Translation of LGPD quoted from: https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/.

Despite this convergence, the implementation of National Civil Identification public policy shows that there is a certain opacity as to how personal data used for citizens' identification and authentication are processed on gov.br platform.

This difficulty reflects some of the LGPD's provisions, especially those concerning the public authorities' personal data processing. The law's art. 23-I states that legal entities governed by public law shall be authorized to fulfill legal obligations serving the public interest, provided that:

> I – they communicate the situations in which, in the exercise of their regulatory capacities, they carry out the processing of personal data, supplying clear and up-to-date information about the legal base, purpose, procedures and practices used to carry out these activities in an easily accessible media, preferably on their websites;[33]

For the same requirement of publicity and therefore transparency of the public authorities' personal data processing as a duty of the Public Administration, the National Data Protection Authority (ANPD)'s Guidance for Personal Data Processing by the public authority, shows that the Digital Government Law (Law 14.129/2021) establishes specific measures for publicity and transparency of the public authorities' personal data processing activities in order to materialize data subjects' rights enumerated in the LGPD's art. 18. Per the Digital Government Law's art. 25:

> Art. 25. Digital Government Platforms **must have transparency and control tools for personal data processing that are clear and easily accessible to enable citizens to exercise rights stipulated in Law No. 13.709 of August 14, 2018 (General Personal Data Protection Law).**
>
> § 1 Tools stipulated in this article's header must:
>
> I - provide, among other details, the sources of personal data, the specific purpose of their processing by the respective body or entity, and indications of other bodies or entities with which personal data are shared, including their history of shared access or use,

33 TN6: Translation of LGPD quoted from: https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/.

except for cases stipulated in of the caput of Law No. 13.709's art. 4 - III of August 14, 2018 (General Personal Data Protection Law);

II - allow citizens to submit requests to the body or entity controlling their data, especially those stipulated in Law No. 13,709's art. 18 of August 14, 2018 (General Personal Data Protection Law).

§ 2 The National Data Protection Authority (ANPD) may publish supplementary rules to regulate the provisions of this article. (BRAZIL, 2021c, our emphasis)

This means that there is an expectation of the publicity of state acts, in order to encourage the creation of:

> a kind of active citizenship, typical of republican models since it allows citizens to control public activity and in particular oversee the management of public affairs. In this respect, Daniel Sarmento (2014, p. 2017, apud MULHOLLAND, MATERA, 2020, p. 225) states that 'republicanism emphasizes the importance of the public sphere as a place for exchanging reasons, exercising the important role of supervising the concrete functioning of formal political institutions' (MULHOLLAND, MATERA, 2020, p. 225).

Given these provisions, the duty of state transparency may be incompatible with the National Civil Identification System as it is. This tension is justified by the fact that the federal government does not facilitate citizens' access to documentation that addresses both the purpose of the data processing activities involved in National Civil Identification and the personal data processing procedures and techniques used by ICN and the user authentication service for the gov.br platform. So there is a risk of data subjects' exercising their rights being difficult or even impossible, as well as civil society auditing and inspection of the aforementioned public policies. The purpose of the rights enumerated in the LGPD's 18 is to enable data subjects to manage their own data (SILVA, 2020), in order to achieve information self-determination, which is one of the cornerstones of Brazil's personal data protection.

For the purposes of this document, the data subject rights are stipulated in art. 18-I, II and III will be addressed which correspond to confirming the existence of processing,

accessing data and correcting incomplete data.

Silva (2020) argues that the right to confirm the existence of data processing stipulated by the LGPD's art. 18-I derives from the principle of transparency, and must be upheld without any opposition from the processing agent, since

> the absence of data processing confirmation prejudices assurances of other rights, especially considering cases in which the requirement invoked for data processing is not consent; in these situations a data subject may only become aware of data being collected if and when the person responsible for processing confirms it (SILVA, 2020, p. 196)

The right to access data is stipulated in the LGPD's art. 18-II is a logical development from the right to confirm data processing, therefore the purpose of a data subject exercising this right is to see how their data have been processed (SILVA, 2020), in other words, whether data are being processed securely and fulfilling their purpose.

In this respect, Silva (2020) argues that the right to access data arises from the principle of free access, which is characterized by "guarantee to the data subjects of facilitated and free of charge consultation about the form and duration of the processing, as well as about the integrity of their personal data" (BRASIL, 2018), per the General Data Protection Law's art. 6-IV.

Likewise, the right to correct incomplete data is derived from the principle of data quality addressed in Chapter 3, section 3.3c of this document. Ensuring that data are updated is crucial to fulfill the purpose of a certain personal data processing activity, especially those taking place in the context of implementing public policies such as National Civil Identification and the use of its database to authenticate gov.br platform users. In view of the right to correct incomplete data, good practices for processing data must include keeping historical records of changes and updates to broaden the data subject's access to information (SILVA, 2020).

Here, the opacity identified in the public policy for user authentication on the gov.br platform, based on using the ICN's database, has the potential to prevent personal data subjects from exercising their rights. This potential may be identified in the absence of a suitable direct channel of communication for citizens to request confirmation of the existence of data processing, get access to their processed data, and rectify any incorrect and/or outdated data.

4. Risks of excluding citizens from access to public services on gov.br

The objective of this chapter is to analyze social vulnerabilities that may lead to the exclusion of citizens from accessing public services on gov.br due to the authentication procedure based on ICN's database. Therefore, this section will explore the second main category of risks arising from structuring the identification public policy that has been mapped in this research.

As Chapter 2 of this report noted, one of the objectives of the Digital Government Strategy is digitizing public services - and gov.br is central for this task. Considering this objective, the possible consequences of automating public services for the most socially vulnerable must be kept on the horizon. As Eubanks (2018) warns, the use of automated systems to manage public services - particularly those related to social benefits and managing poverty - may further exclude socially marginalized groups and prevent the most vulnerable from accessing social services.

Eubanks (2018) drew this conclusion from an empirical investigation of cases in the United States, from which she shows how automated systems did not boost the efficiency of services or reduce fraud - the assertions and defenses usually used as pretexts when implementing these systems. On the contrary, their spread has exacerbated existing socio-economic vulnerabilities and the marginalization of people who were already marginalized. She argues that automated systems are a form of digitized "poor houses", a reference to buildings in the United States where the most socially vulnerable were confined as a matter of public policy from the 17th through the 20th century - where their lives were managed but their poverty was not eradicated. Although the American case researched by Eubanks deals with a different geographic reality and different public policy instruments, the reasons for exclusion arising from automated decision-making, such as social vulnerabilities, racism, disabilities, exclusion of children and adolescents, and difficulties handling documentation issues are also frequently reported in Brazil. In this respect, this section briefly portrays vulnerabilities that may lead to people being excluded from the ICN's databases (collectively referred to as BDICN), or from using gov.br, although they do not seem to have been considered when these public policies were designed.

Analyzing social vulnerability is a fruitful way of looking at the exclusion scenario in Brazil, where social vulnerability involves structural inequalities rooted in society and

poverty has been gendered and racialized: black women remain in the poorest strata of the population. Before the novel coronavirus pandemic started in 2019, 33% of black women were below the poverty line; by 2021 this number rose to 38%, so on a similar level to black men. Meanwhile, for white women and men, 15% were below this line before the pandemic, rising to 19% in 2021 (ROUBICEK, 2021).

The factors that lead to social vulnerability may also be combined, as described by Escóssia (2019), who found that a disproportionate number of black women lacking identification documents were living in poverty or extreme poverty.

4.1. Exclusion due to inadequate identity documents

a. No identity document

The Brazilian authorities will not issue an identity document unless the citizen in question has previously obtained a birth certificate. To refer to people who have no registered birth certificate, the IBGE uses the term under-registration, meaning the number of births that have not been registered by year-end or by the first quarter of the subsequent year they ocurred (IBGE, 2020). The number of adults currently going through life without a birth certificate is unknown, so these individuals are invisible to the State (ESCÓSSIA, 2019).

To get their personal data registered in the ICN's database, an individual must first obtain an identity document, driver's license or voter registration card, none of which will be issued unless they have previously had a birth certificate issued. So, birth certificates are called "foundational documents": until a citizen has one, they will be unable to get any other document – usually the first one, after the birth certificate, is an identity card produced by extracting information from a civil registry, adding biometric records and collecting fingerprints (ESCÓSSIA, 2019). If a citizen does not have a birth certificate, their personal data will not be registered in the ICN database so they will be unable to access gov.br or the public services available there.

Since the late 1990s and throughout the 2000s, governments have been holding campaigns to eradicate under-registration. Especially relevant among them was one that involved issuing birth certificates free of charge under Law No. 9.534/1997 (IBGE, 2020). Before that, back in 1990, the estimated under-registration rate was 29.3%. By 2002, the number had fallen to 20.3% and more recently 2017 data show 2.6% of total birth were not registered (VILAS BÔAS, 2019; ESCÓSSIA, 2019). However, although the percentage

is falling, an important point to note is that the rate is unevenly distributed across the country, being higher in the North (9.4%) and Northeast (3.5%), the country's poorest regions (VILLAS BÔAS, 2019). In this situation, the poorest and oldest are more likely to be unregistered and therefore excluded from the ICN's database and unable to access public services through gov.br.

To portray the phenomenon of adults without birth certificates, Escóssia (2019) conducted an ethnographic survey of users of a public service that was issuing birth certificates free of charge for people without registration. This initiative is the result of a partnership between two projects sponsored by the State of Rio de Janeiro's Court of Justice (TJRJ): one was dubbed 'itinerant' or 'traveling' justice, and the other was the Service for Promotion and Eradication of Birth Sub-Registration and Obtaining Certificates (Sepec). These users had no documentation at all until they contacted this service, and the author explored the duality between the document as key for state control, but also to access to rights - a duality that has also been explored in this policy paper. People who do not have birth certificates do not have any other documents either, so they cannot vote, get a formal-sector job, or open a bank account or own any goods or assets in their own name. They can only get health care if there is an emergency; and schools also require documentation to enroll children (ESCÓSSIA, 2019).

Escóssia's observations showed that most unregistered people had some shared characteristics, such as their race/ethnicity (black or brown), female gender, and poverty or extreme poverty. Another relevant aspect is that not having registration was often generational: if a mother does not have a registration, she cannot register her children (ESCÓSSIA, 2019), thus starting a cycle of exclusion that is hard to break:

> Under-registration is still a problem associated with social exclusion and a different variant of citizenship - to which part of the Brazilian population is subjected. Very low-level education, being short of money, underemployment and poor financial and social standing, often in situations of poverty and illness, eventually transform an undocumented adult into a citizen with low levels of autonomy and ability to enter the world of work. Such is the outcome of citizenship built on being denied rights or afforded only marginal access to rights. This, a passive, patient type of citizenship shaped by red tape or what she calls the counter syndrome (being shuttled from one line to another to talk to officials), and not in a hurry to assure others' rights (ESCÓSSIA, 2019, p.82).

Escóssia (2019) observed users of the free public service issuing certificates and found that they had different motivations for obtaining birth registration, which could be multiple for the same person. A frequent reason was accessing public policies and social benefits, especially Bolsa Família, which required a birth certificate, identity document and taxpayer number (CPF), including of the family's children. Another reason was an event that required attendees to get an ID document urgently, as in the case of Maria, a service user who had a malignant breast tumor that could only be operate on and treated if she submitted her ID documents. Escóssia called the third reason 'conversion': when a person's life's trajectory is riddled by abusive alcohol and drug use, and they had no documents or had lost them. As part of changes in their lives, while being treated for abuse, they sought to recover their documents or get them for the first time. Finally, there were people who sought a more intangible feeling of learning their origins and family history from their ID document (ESCÓSSIA, 2019)[34].

The gov.br website can only be accessed by using a login or username that depends on the citizen's being registered in the ICN's database, so a person that does not have an identity document will not be able to access public services on gov.br, thus excluding part of the population. One way of avoiding exclusion would be entering without a login to access information from the available services, combined with information on how a citizen may act if they are not registered with the ICN or if they do not have civil identification documents.

b. Inadequate identity document

In addition to not having an identity document, there is also a risk of being excluded from access to public services on gov.br for citizens whose ID document does not match their gender identity, which is the reality for many transgender people in Brazil. Note that this population is extremely vulnerable on the national level: Brazil has the world's highest number of murders of trans people (LOPEZ, 2020; SUDRÉ, 2020). If a person's ID document does not match their gender identity, they will be discriminated when accessing public services, since they will have to use their registered name, which may even lead them to avoid attempting access.

34 One of the merits of Escóssia's study is giving voice and life to aspects normally seem as just numbers, such as under-registering. People who do not have an identity document lead vulnerable lives in relation to the State. The story of Maria Cristina de Oliveira, born in Miguel Alves (PI), is told in Revista Piauí (LIMA, 2022). In January-February 2022, after giving birth, Maria remained in Promorar municipal hospital's maternity ward for thirty days. She had no ID document and had not been registered, so the hospital refused discharge, despite the absence of any legal provision in this respect.

There are two ways for a transgender person to get ID documents that reflect their gender identity: one of them is taking the administrative route to change them at a civil registry office, once they reach the age of 18, a service for which they must pay. The other is using their social name. Having a social name for filling in forms and official records is obviously important, according to a Trans Persons Mapping project in the municipality of São Paulo, using a social name to fill out records and forms happened 83% of the time for trans women, 80% of the time for transvestites and 72% of the time for trans men (CEDEC, 2021). Unlike other public service registries, such as those attached to the Ministry of Education (MINISTÉRIO DA EDUCAÇÃO, 2017) and Health (MINISTÉRIO DA SAÚDE, 2009), the ICN does not have a "social name" field, which allows the person to be identified by the name they use and are socially recognized by rather than their registered name. Problems involving social name fields, with discriminatory consequences for the rights of trans people, have arisen with government digital records such as Cadsus in January 2022 (DAMASCENO, 2022).

Social names are also relevant for transgender children and adolescents, whose registration can only be rectified by a court order. A survey conducted by the Caribou Digital NGO in 2020 found that there is a conflict between how Brazilian children and young people define their own gender identities and their static identity defined at birth, which will, as a rule, be the one registered in the BDICN.

In the case of transgender people, therefore, the BDICN would have to be adapted to, at least, add a 'social name' field, thus enabling their non-discriminatory access to public policies.

4.2. Exclusion of hypervulnerable subjects: children and adolescents, persons with disabilities, and seniors

a. Children and adolescents

The Federal Constitution's article 227 and the Children and Adolescents Statute's article 4, sole paragraph, subparagraph (c), assure children absolute priority to access rights through public policies. Concurrently, the UN Committee on the Rights of the Child[35], in the General Comment 25 regarding the digital environment, suggests that States should

35 For the UN, under the Convention on the Rights of the Child, individuals under the age of 18 are considered children. For Brazil's Children and Adolescents Statute, individuals aged twelve or less are children while those aged from twelve to eighteen years of age are adolescents.

promote the use of digital identification systems that include birth registration for all newly born. It also requires States to ensure recognition of these records by national authorities to ensure children's access to services such as education or social welfare and sees the absence of registration as facilitating rights violation (as addressed above in 4.1.1's under-registration section).

Despite these legal provisions, two of the ICN's main databases - Electoral Court and State Government Traffic Department databases - do not contemplate children or the great majority of Brazilian adolescents: only adolescents aged over 16 may be in the Electoral Court's database and only over-18s in Detran's. There are no articles specifically for children and adolescents in the ICN Law.

Children and adolescents must be respected and have access to rights depending on the stage they have reached in their development. They must also be assured of access to public services through gov.br using age-group appropriate means. Any operation involving data of subjects aged under 18 must be structured differently to protect the specific vulnerability applicable to this group and their assured constitutional and legal protections, but an important aspect of their status as citizens is that they are covered by the National Civil Identification.

b. Seniors

The Seniors Statute's article 3 assures over-60s of absolute priority to access rights and protection for aging as a social right.

Research conducted by Sesc São Paulo and the Perseu Abramo Foundation in 2020 found that seniors generally feel excluded from the digital world and have difficulty reading. Some 40% of the seniors in the survey sample reported some kind of reading and writing difficulty due to a lack of basic education, illiteracy, or functional illiteracy. Moreover, only 19% used the Internet effectively, and 72% of this demographic said they had never used an app, while 62% had never used social networks (BOCCHINI, 2020)[36].

Due to difficulty reading and using the Internet, seniors may be largely excluded from using gov.br and accessing public services. Therefore, a specific policy is to be recommended and it should be designed for this demographic segment to access and use public services in order to be effectively digitally included.

36 Survey of 2,369 people aged over 60 covering all five of the country's regions, with a margin of error of up to 2.5 percentage points.

c. People with disabilities

The rights of people with disabilities are stipulated in the specific legislation, the Persons with Disabilities Statute (Law No. 13.146/2015) to "assure and uphold in conditions of equality, the exercise of fundamental rights and freedoms for people with disabilities, and their social inclusion and citizenship" (BRASIL, 2015).

The gov.br platform adds two mechanisms to enhance its accessibility: high contrast and Brazil's Libras sign language. However, not all authentication technologies used on the platform are necessarily accessible for all audiences. There have been reports of visually impaired users having greater difficulty with facial recognition tools and in some cases needing outside resources to help them, such as vibrations on devices or voice commands in addition to a specific algorithm designed to contemplate their needs (KEANE, 2016).

Another problem that may arise for people with disabilities relates to the use of biometrics, which entails registering their fingerprints. The layouts of devices used to capture and read biometrics assume that users' bodies conform to a standard model - which does not exist - and there are limitations in terms of the size and position of scanners, so people with disabilities in their upper limbs may have difficulty getting their fingerprints scanned.

The LICN does not contain specific articles for people with disabilities or on ways of ensuring their inclusion in its database on equal terms. Nor does the gov.br platform's structure appears to incorporate concerns of this type. So, using BDICN to access public services through gov.br poses a risk of discrimination and exclusion for people with disabilities.

4.3. Exclusion due to no Internet access or difficult Internet access

Another case of exclusion arising from the current structuring of authentication services used to access public services via gov.br concerns Internet access issues, a situation that prevents citizens from using the portal, which is only available online, for smartphone or desktop users.

Brazil's Households Survey (TIC Domicílios) (2021) reports that the proportion of households with Internet access reached 83% in 2020 and was 12 percentage points higher than the previous year. This trend was more pronounced in the most vulnerable socio-economic strata, especially classes C (access rose from 80%, in 2019 to 91% in 2020) and

D-E (access rose from 50% in 2019 to 64% in 2020). In population-wide terms, an estimated 81% of those aged 10 or more used the Internet in 2020, up seven percentage points from the previous year, and the highest growth was in the most vulnerable socioeconomic strata, i.e. classes C (from 78% to 85%) and D-E (from 57% to 67%) (CETIC.br, 2021).

These numbers indicate quite substantial progress for Brazilian society, but at the same time shows that 19% do not use the Internet. These people would be excluded from using the gov.br service. Furthermore, an important aspect to note is that the number of households with Internet access in classes D and E is significantly lower than the average - 67% versus 83% - which shows that the greater the social vulnerability, the greater the chance of not having Internet at home and having more difficulty accessing digitized public services on gov.br. Regional inequality also affects access (IDEC, 2022), which suggests a probable disproportionate distribution of access to platform services: the Northeast region has the lowest percentage of households with access (79%) while the Southeast region has the highest (86%). Other regions surveyed reported the following household Internet access levels: North (81%), Mid-West (81%), and South (84%) (CETIC.br, 2021).

Together with the reported rising Internet access levels for the most vulnerable socioeconomic strata, data for 2019 - 2020 showed a higher proportion (from 28% to 42%) of users searching for information offered by government websites. The proportion accessing public services through the Internet was also up (from 28% to 37%). However, an important issue to be emphasized is that the numbers are still low: only a minority use internet for these activities. Furthermore, note that these online activities were more frequent among users in urban areas (39%), class A (63%), and the college-educated (68%), both groupings that previously had already been involved in wide-ranging Internet-related activities (CETIC.br, 2021), thus showing a trend that, were it applied to gov.br, would exclude the most vulnerable users from the platform.

Again, in terms of Internet access, in 2020 as in 2019, cell phones were still the devices most often used by almost all Brazilians aged 10 or more that access the digital environment (99%). For more than half of the users who use a cell phone as their main device (58%), access was exclusively through this device, and this proportion rises to 90% for those who had only early childhood education or belong to classes D and E (CETIC. br, 2021). Using only cell phones to access the Internet was also reported more often (65% and 60% respectively) among those who described themselves as black or brown (pardo) and those living in the Northeast region (72%) (CETIC.br, 2021); these data show that the greater the social vulnerability, the greater the exclusive use of cell phones for Internet access.

On the same lines as these findings, a survey conducted by the Brazilian Institute for Consumer Protection (Idec) and Instituto Locomotiva (2021) examined Internet access for socioeconomic strata C, D and E. Their findings show that most people used their cell phones to access the Internet (91%) and the majority used their own 3G/4G cellphone network to access the Internet (90%). In relation to access to electronic government services, the survey found that 39% had at least once not had access to public policies because their smartphone had no Internet connection, 33% had at least once not accessed public services and 28% had at least once not accessed social benefits such as emergency assistance (cash benefit during the Pandemic for the needed). This is directly related to the fact that the individuals interviewed had accessed the Internet on an average of 23 days in the previous month; for the rest of that time, their Internet was blocked due to not paying for additional use.

All these findings show higher levels of vulnerability in the CDE socioeconomic strata in relation to internet access. Even when citizens get past the Internet access hurdle, they will not necessarily be able to use suitable devices to usefully browse the net or be able to afford an always-on connection, so they too have trouble using digital government services. In other words, access to gov.br is still behind large barriers for the most socially vulnerable groups, which may lead to their exclusion from the public services offered on this platform. To mitigate this type of exclusion, two measures are simultaneously recommended: (i) firstly, there should still be physical channels available to register for public services and access them, and their quality should be at least the same as digital media services; and (ii) secondly, there should be more investment in public policies to fully universalize high-quality Internet access.

5. Addressing risks for fundamental rights and civil liberties: accountability measures and Data Protection Impact Assessment

5.1. The "riskification"[37] of personal data protection

This report's previous chapters sought to outline certain implications of the current information and governance structure for Brazil's National Civil Identification system, as well as risks arising from using it to authenticate users on gov.br for their access to federal public services offered through this platform.

In this respect, the element of risk takes on a key role in the analyses covered by this document, so this aspect should be interpreted in structural terms. Raphaël Gellert (2016) suggests approaching the notion of risk through two definitions: (i) its literal definition; and (ii) its technical conception.

From a literal perspective, the risk may be interpreted as the possibility of future hazard or danger. Meanwhile, a technical conception interprets risk from a double point of view: its use for decision-making processes, based on the evaluation of future events. So Gellert (2016) argues that risk involves two elements that are distinct but jointly operationalized: predicting future events, be they favorable or adverse, and decision-making based on this prediction. From this point of view, personal data protection laws may be seen as one of several tools for the governance of risk arising from Information and Communication Technologies (ICTs) (GELLERT, 2015).

On the same lines, Claudia Quelle (2015) notes that precisely the latest-generations personal data protection laws have to an even greater extent built in a risk-based approach, as the element that calibrates legal obligations so that the weight of regulation will correspond to the level of the adversity involved (QUELLE, 2015).

Based on these premises, according to Rafael Zanatta (2017, p. 9), personal data protection "riskification" means that its material consists of the following elements:

37 The concept of riskfiying personal data protection was first coined in Alessandro Spina's "A Regulatory Mariage de Figaro: Risk Regulation, Data Protection, and Data Ethics", an article published in the European Journal of Risk Regulation in 2017 (SPINA, 2017).

> (i) collective class action instruments and participation of civil entities in a preventive dialogue with independent personal data protection authorities, (ii) ex ante obligations and regulatory instruments attributed to controllers to identify risks affecting fundamental rights and freedoms, (iii) the spread of "risk management" methodologies and calibration between risks caused by personal data processing and use and legal immunities constructed by ethical discussion around technical progress and its limits.

This riskification process is relevant to the extent that precautionary measures applied in personal data protection governance are again debated and replace the previous method of responding to any harm or damage by focusing solely on regulatory mechanisms for punishment and reparation (*ex post*). In Brazil's personal data protection context, discussions around precautions and *ex ante* regulatory measures are materialized by the accountability principle[38-39]. The Brazilian General Data Protection Law's article 6-X defines this principle: "X – accountability: demonstration, by the data processing agent, of the adoption of measures which are efficient and capable of proving the compliance with the rules of personal data protection, including the efficacy of such measures." (BRASIL, 2018)[40]. In this respect, Bruno Bioni and Maria Luciano state that:

> the precautionary principle shows two regulatory directions that deserve attention: a) the regulatory debate being opened up to all actors involved in the implementation of this technology (and in the choices thus required), from developers to those who will feel its possible effects, which is a mandatory requirement of a democratic system that has historically been characterized by power and information asymmetries; b) attributing obligations to reduce uncertainties around the benefits and risks in question (...).
>
> In this respect, general personal data protection laws (..) introduce a precautionary tool to be analyzed. Its calibration will vary on

38 For the purposes of this document, the expressions "accountability" and "held to account and rendering accounts" will be used interchangeably as synonyms.

39 The Information Commissioner's Office (ICO) describes accountability as one of the personal data protection principles that addresses the responsibility of a given organization to comply with personal data protection legislation, as well as its ability to document said compliance. For more details: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/#whataccountability

40 TN7: Translation of LGPD quoted from: https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/.

> the scale across low, moderate, and high in terms of the level of prudence (...). Unlike paralysis or inaction, personal data protection impact assessments, audit mechanisms and conversations with regulatory bodies and other affected actors are actions that may serve as a conscious and responsible driving force for launching this technology in the environment (BIONI, LUCIANO, 2019, p. 19, our emphasis)

In this scenario, personal data protection impact assessments - also known as DPIAs - emerge as one of the main precautionary tools for ex ante regulation and accountability in the development of policies and activities involving personal data processing.

5.2. A "General theory" of Data Protection Impact Assessments[41]

Impact assessments are not governance tools. They emerged from the need to lend a certain degree of certainty to uncertain events, from the emergence of new hazards for society on individual and collective levels (KLOZA *et al*, 2020)[42]. In other words, impact assessments, according to Kloza *et al* (2020, p. 2) are tools used to examine:

> how possible consequences of an initiative may affect a relevant social interest or interests if this initiative could endanger these interests. This tool supports informed decision-making processes as to whether the initiative should start and, if so, on what conditions, ultimately translating into a means of protecting the above-mentioned social interests.

According to Kloza *et al* (2020), impact assessments in areas such as healthcare, regulation, and personal data privacy and protection were developed from positive experiences of compiling these documentations for other areas, such as the environment.

In personal data protection terms, the more widespread use of Privacy Impact Assessments (PIAs) – precursors of Personal Data Protection Impact Assessments (DPIAs) - as of

41 Note beforehand that Personal Data Protection Impact Assessments are the European instruments' equivalent to the personal data protection impact reports established by the Brazilian General Personal Data Protection Law.

42 Note that this article was originally published in 2017 before Brazil Data Privacy Research Association published a Portuguese translation in 2020 as the result of a partnership between Data Privacy Brasil and d.pia.lab – Brussels Laboratory for Data Protection & Privacy Impact Assessments attached to Vrije Universiteit Brussel (VUB).

the 1990s may be related to three factors:

> (1) the increasingly invasive aspects of emerging technologies for the lives of individuals and the social fabric; (2) the growing importance of personal data processing for the contemporary economy, national security, scientific research, technological development, interpersonal relationships, and other sectors, and (3) diminished trust or confidence in emerging technologies and their use by the public and private entities (KLOZA *et al*, 2020, p. 2)

In this respect, Clarke (2009) addresses Privacy Impact Assessments and emphasizes that PIAs - and this goes for DPIAs too - are distinguished from other organizational activities such as complying with data protection legislation, especially due to their ex-ante nature, i.e. due to the fact that they are compiled prior to data processing.

Clarke, therefore, posits certain fundamental elements for characterizing Privacy Impact Assessments, in particular the following : (i) PIAs must be conducted with a project or initiative in mind, differing from an organizational privacy strategy; (ii) the nature of PIAs is anticipatory since they must be conducted before or along with the development of a given activity; (iii) privacy impact assessments have a broad scope, which must take into account subjects affected by a given data processing activity; (iv) PIAs must address both the problems (risks) of activity and solutions to these problems; and (v) PIAs are processes that require entire organizations to be intellectually engaged.

In dialogue with Clarke (2009), Kloza *et al* (2020) state that compiling an impact assessment – and in the context of this report, a personal data protection impact assessment – has twofold advantages: assisting the process of making informed decisions based on risk assessment and protecting social interests.

In relation to the first advantage, there is a visible shift from regulatory rationality toward anticipatory (ex ante) thinking. Kloza *et al* (2017) suggest that this shift prompts both public and private sector organizations to start thinking about the consequences arising from a certain data processing activity. This process of reflection leads to higher levels of public trust since there is an active search for ways of minimizing or even avoiding the adverse consequences of the operations to be undertaken (KLOZA *et al* 2020).

Concerning the first advantage, moreover, Kloza *et al* (2020) emphasize that compiling personal data protection impact assessments would assist the compliance process - although not being confounded with the latter - and demonstrate accountability for regulatory agents.

As to the advantage of protecting social interests, personal data protection impact assessments on individual and collective levels do help protect socially relevant interests, such as human rights. After all, their purpose is precisely mapping and foreseeing measures to mitigate data processing adversely interfering with data subjects' rights. In this respect, personal data protection impact assessments may help to strengthen procedural justice, whose pillars for the assessment concept itself consist of participation (voice), neutrality, respect, and trust (TYLER, 2008, pp. 30–31 *apud* KLOZA, 2014, p. 4).

Compatibility between these pillars and the nature of the ex-ante documentation discussed here is more easily verifiable in relation to the principle of participation. By allowing individuals to voice "their concerns (e.g. through social participation)" (KLOZA *et al*, 2020, p. 3), DPIAs could strengthen the idea of procedural justice, since the principle of participation would be upheld (KLOZA, 2014).

Another crucial point in this area is realizing that personal data protection impact assessments start from the notion of the right to personal data protection being autonomous in relation to the right to privacy. This autonomy was shown when the European Union General Data Protection Regulation (GDPR) was promulgated. This regulation's article 35 expressly stipulates personal data protection impact assessment:

> Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, **is likely to result in a high risk to the rights and freedoms of natural persons**, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks[43].

The General Personal Data Protection Regulation relates DPIAs to the existence of high risk for data subjects' civil rights and fundamental freedoms per article 35, No. 1, and poses them as the focal point to which impact assessment should be directed. Therefore, it is the activity's high level of risk that triggers a personal data protection impact assessment.

In addition to relating a DPIA to the existence of a data processing operation that is likely to result in a high risk for data subjects, the GDPR lists certain situations, although not

43 TN8: Direct quote from: https://gdpr.eu/article-35-impact-assessment/.

exhaustively, in which an impact assessment must be performed:

> 3 a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
> (b) processing on a large scale of special categories of data referred to in Article 9(1), or of personal data relating to criminal convictions and offences referred to in Article 10;
> c) Or a systematic monitoring of a publicly accessible area on a large scale[44].

Along with these situations, the Article 29 Working Party on Data Protection published "Guidelines on the Data Protection Impact Assessment (DPIA) which determine whether processing is likely to result in a high risk for data protection purposes of the Regulation (EU) 2016/679". It was published in 2017 before the European Regulation on Personal Data Protection came into effect - but after its approval - and the guidelines aim to resolve the subjective nature of the notion of "high risk".

According to these guidelines, compiling a DPIA is especially important when a new data processing technology is implemented. They also recommend compiling DPIAs even in situations in which there is no obvious mandatory requirement since these assessments are fundamental instruments to help processing agents comply with data protection legislation (ARTICLE 29 DATA PROTECTION WORK GROUP, 2017).

The document also highlights the fact that the GDPR includes a non-exhaustive list of activities that may involve high-risk data processing, so there may be other types of activities covered by this category. In other words, the Regulation allows National Data Protection Authorities to draw up lists of processing operations that may pose a high risk to data subjects' rights and freedoms. Per Article 29 Working Group guidelines (2017, p. 10-12), the lists must meet nine criteria, some of which are already included in Article 35 - No. 3, of which the following are : (i) when there are automated decisions that produce legal effects or similarly affect the natural person; (ii) when there are sensitive data of a highly personal nature; (iii) when data processing relates to vulnerable data subjects, who may include children, employees, more vulnerable segments of the population who need special protection, and all cases in which imbalance between the data subject's and

44 TN9: Direct quote from: https://gdpr.eu/article-35-impact-assessment/.

processing agent's positions may be identified; and (iv) when data processing prevents data subjects from exercising a right or using a service or contract.

5.3. Personal Data Protection Impact Assessment in Brazil

Impact assessments are not foreign instruments for the Brazilian legal system, there has been a legal provision in the Federal Constitution's article 225-IV and the Regulatory Agencies Law's article 6 (Law 13.848/2019) for their conduction (BIONI, RIELLI, 2020). The General Data Protection Law (LGPD) was voted in 2018, so Brazil finally has a legally approved instrument similar to the personal data protection impact assessment. Like the European tool, the DPIA is conceptualized per the LGPD as:

> XVII – data protection impact assessment: documentation from the controller that contains the description concerning the proceedings of the personal data processing that could pose risks to civil liberties and fundamental rights, as well as measures, safeguards and mechanisms to mitigate said risk;[45]

In consonance with what has been called a "general theory" of data protection impact assessments, the DPIA's aim is to be a tool capable of mitigating risks for data subjects' fundamental rights and civil liberties. According to Gomes (2019), based on the definition of the impact assessment in the LGPD's article 5-XVII, two types of risks that should be covered by the instrument may be identified: (i) risks to civil liberties; and (ii) risks to fundamental rights. Here, fundamental rights are those that are set forth in the Federal Constitution's article 5, and as civil liberties, the freedoms of religion, expression, thought and association (GOMES, 2019).

According to Bioni and Rielli (2020), although the Brazilian personal data protection legislation does add some clarification concerning the DPIA, it is not enough. According to the authors (2020, p. 35), in addition to "mentioning the possibility of a DPIA being compiled or required by the Authority (e.g. article 4, §3; 10, §3 and 32), the only slightly more robust provision for this instrument appears in article 38 (...)", in which paragraph 1 stipulates the minimum contents of a personal data protection impact assessment.

45 TN10: Translation of LGPD quoted from: https://iapp.org/resources/article/brazilian-data-protection-law-lgpd-english-translation/.

Other than the abovementioned provisions, Brazil's LGPD has not established minimum procedures required for DPIA, neither for the notion of risk as DPIA triggering element (GOMES, 2020; BIONI, RIELLI, 2020. p. 34), nor for elements relating to the methodology that should be used to compile reports.

Although the purpose of this policy paper is not directly related to discussions of methodologies used to compile data protection impact assessments, their important role must not be ignored. In this respect, Gomes (2020) notes that the methodology used to compile an impact assessment is as important as the assessment itself. There are several methodological possibilities for a DPIA, such as the cost-benefit methodology. However, as Gomes (2020, p. 17) notes: "any methodology that is applied must have rationale grounds and theoretical framework".

On methodologies used to compile DPIAs, this author also notes the essential aspect of understanding that "(...) the referential framework for this methodology is the data subject itself, so the final product is the documentation measuring risks to data subjects' civil liberties and fundamental rights". (GOMES, 2020, p. 17)

On this point, it is worth mentioning Direct Action for the Declaration of Unconstitutionality (ADI) 6387[46]. This action brought by the Federal Council of the Brazilian Bar Association (OAB), sought to declare the unconstitutional status of Provisional Measure (MP) No. 954/2020, which authorized the "obtaining of personal data from consumers of telecommunication services (landline and mobile phones)" (BIONI, 2021, p. 102) in order to enable the Brazilian Geography and Statistics Institute (IBGE) to conduct a Nationwide Household Sampling Survey (PNAD). During her review of the ADI, on proffering a decision on the application for a Precautionary Measure, Judge Rosa Weber highlighted the anticipatory nature of the data protection impact assessment - which she referred to as a "data security impact assessment" and added that a report should be compiled before starting a data processing operation.

In the Brazilian regulatory context, Gomes (2020) believes that the National Data Protection Authority will take up an important role in DPIA regulations, as guidelines on the subject should be issued. Per article 57-J of the General Data Protection Law and in accordance with its powers established by Decree No. 10,474 of 2020, the ANPD announced its regulatory agenda for the 2021-2022 biennium in Order No. 11 of January 2021 (ANPD, 2021), and precisely, made data protection impact assessment one of its priorities for the

46 Bioni (2021) states that these ruling was responsible for a paradigm shift in the jurisprudence of the Supreme Court (STF), recognizing data protection as an autonomous right and a fundamental right.

period.

The first stage of its regulatory process was scheduled for the first half of 2021. By the time of writing this document (May 2022), the Authority had held technical meetings to gather input on the subject. Matters pertaining to DPIA governance addressed at technical meetings attended by experts included the need for sound methodology (GARROTE *et al*, 2021).

Although the DPIA regulation process has not yet concluded here, Brazil's National Data Protection Authority examined the application of the General Data Protection Law to small-scale processing agents (Resolution Cd/ANPD No. 2 of 2022) and started by outlining what is meant by "high-risk data processing activities for data subjects" (ANPD, 2022). The Resolution's article 4 defines high-risk processing as one that cumulatively meets at least one of the general criteria and one of the specific criteria, as shown below:

> Article 4 For the purposes of this regulation, and without prejudice to the provisions of article 16, personal data processing that cumulatively meets at least one general criterion and one specific criterion, from among those shown below, shall be considered high risk:
>
> I - general criteria:
>
> a) **large-scale personal data processing; or**
> b) **personal data processing that may significantly affect data subjects' interests and fundamental rights;**
>
> II - specific criteria:
>
> a) use of emerging or innovative technologies;
> b) surveillance or control of areas accessible to the public;
> c) **decisions made solely on the basis of automated personal data processing, including those used to define the personal, professional, healthcare, consumer and credit profile or aspects of the data subject's personality;** or
> d) **use of sensitive personal data or personal data of children, adolescents and seniors.**
>
> § 1 Large-scale personal data processing shall be characterized as such when it covers a significant number of data subjects, also considering the volume of data involved, as well as processing duration, frequency and geographic extent.

> § 2 Personal data processing that may significantly affect interests and fundamental rights shall be characterized, among other situations, in those in which processing may prevent subjects from exercising rights or using a service or may cause data subjects material damages or suffering such as discrimination, violation of physical integrity, the right to image and reputation, financial fraud or identity theft. (ANPD, 2022, no page numbering, our emphasis).

Furthermore, the Guide to Application of General Data Protection Law (LGPD) for processing agents in the electoral context, authored by the ANPD and TSE, stipulates that the DPIA is an important instrument of accountability in the electoral context, since there may be large volumes of sensitive data such as political opinions and membership data. Also, according to the guide, although the LGPD does not regulate the contexts in which DPIAs must be compiled, DPIA reporting is highly recommended in high-risk scenarios, for example, scenarios involving large-scale sensitive data processing.

According to these indications of the ANPD's understanding of the subject, the data operation involved in the public policies of ICN and gov.br attracts four of the six elements listed to characterize it as a high-risk activity, from general and specific points of view:

General Criteria (Article 4-I of Cd/ANPD Resolution No. 2 of 2022)	**ICN e Gov.br** (High Risk Data Processing)
Large-scale personal data processing will be characterized when there is a significant number of data subjects, also considering the volume of data involved, as well as the duration, frequency and geographic extent of the processing. (Article 4, I, "a", § 1)	The ICN is a state policy for the identification of Brazilian citizens considered invisible to the State. Per content posted on the website of the Superior Electoral Court (TSE), updated May 17, 2022, there are more than 118 million people whose biometric identification has been registered with the Court; this number corresponds to about 80% of Brazil's electorate (TSE, 2022b). Gov.br plans to digitize and expand access to public services. Federal government data show that the gov.br platform had 57 million unique users in February 2022 (GOVERNO FEDERAL, 2022)[47].

47 These same data note a 19% increase in the total number of unique users in relation to January 2022.

Personal data processing that may materially affect data subjects' interests and fundamental rights, which will be characterized, among other situations, in those in which processing activity may prevent the exercise of rights or use of a service, as well as cause material or moral damages to holders, such as discrimination, violation of physical integrity, the right to image and reputation, financial fraud or identity theft. (Article 4, I, "b", § 2)	The purpose of data processing is to identify citizens eligible for a series of rights in the context of their relationship with the State. Briefly, the data processing in question materially impacts a data subject's civil life across a wide range of different spheres and contexts, as well as their access to public services.
Data processing activities in the policies of ICN and gov.br meet the two (02) general criteria required to be characterized as high-risk activities	
Specific Criteria (Article 4, II of Resolution Cd/ANPD No. 2 of 2022)	**ICN and Gov.br** (High risk Data Processing Activity)
Decisions made solely on the basis of automated personal data processing, including those used to define personal, professional, health, consumer, and credit profiles or aspects of a data subject's personality (Article 4, II, "c")	The citizen identification process necessarily involves the use of biographical and biometric data - aspects of the holder's personality - to make him/her unique. Also, in order to enable the large-scale data processing in question, there is a substantial degree of automated ICN flow, as well as a provision in the LICN on cross-referencing citizens' data in order to verify eligibility for social benefits
Use of sensitive personal data (Article 4, II, "d")	A series of sensitive data is processed, including biometric data, so there full individualization of citizens.
Use of personal data of children, adolescents and seniors (Article 4, II, "c")	There is the processing of data from adolescents aged over 16 and seniors, considered hyper-vulnerable per laws 8.069 of 1990 and 10.741 of 2003.
Data processing in ICN and gov.br policies attract all three specific criteria to characterize it as a high-risk activity	

In the current Brazilian regulatory context, ICN and gov.br may now be rated high-risk data processing activities. In keeping with the principle of accountability, these databases' controllers should have prepared data protection impact assessments to demonstrate the efficacy of measures taken to protect the data of a large part of the Brazilian population: an accountability measure that would support the implementation of a national civil identity system and platformed public services strengthening the bond of trust between citizen and State.

a. The public sector and publicized data protection impact reports

As mentioned above, a DPIA document originates from a complex process in which risks to the fundamental rights and civil liberties of data subjects arising from a given personal data processing activity are described and assessed. The DPIA process determines risk-mitigating measures, safeguards, and mechanisms, and the core element triggering the compilation of this document is the processing of data resulting in a high risk.

Since the DPIA is a powerful means of ensuring accountability and data subjects' rights, another aspect as relevant as compiling the report is publicizing it.

Once again, the General Personal Data Protection Law has nothing to say on the matter: it does not directly require impact assessments to be publicized, although the LGPD's article 32 does state that the National Data Protection Authority may ask agents of public authorities to publish a DPIA. The takeaway from this provision is that publicizing an impact assessment takes on new aspects when compiling one related to public authorities' power of data processing, as is the case of the National Civil Identification and the use of the National Civil Identification Database on the gov.br platform.

In this scenario, a systematic interpretation of the General Personal Data Protection Law provisions and the Public Administration's constitutional principles leads one to conclude that there is a general obligation for public authorities to publicize DPIAs, since as addressed by chapter 3, section 3.3b, they have the duty of making its data processing public, especially when there are sensitive data and when the legal basis chosen to justify processing is not consent.

This duty also arises from constitutional principles governing Public Administration activity, especially the principle of publicity. Per Carvalho Filho (2020), the principle of publicity states that the public administration's acts must be public and must be widely disclosed to those administered since only transparency for the Public Administration's activities will enable individuals to exert control over the legitimacy of given conduct - in the case in question, control over personal data processing.

Publicizing the Public Administration's actions is therefore directly related to the principles established by the General Personal Data Protection Law, particularly the principle of accountability stipulated in the LGPD's article 5-X to the extent that, when considering the asymmetry of power between the processing agent and the data subject, it ensures that the latter has access to see how data processing activities are conducted, which includes DPIAs.

In this respect, Gomes (2020) warns that publicizing the instrument is directly related to visibility in terms of which methodology is adopted for the purposes of cognizance, assessment, and mitigation of risks to data subjects' fundamental rights and freedoms. In other words, as important or more so than the risk management process itself is disputing it and placing it under public scrutiny so that the report becomes a means of fulfilling its aspirations of safeguarding data holders' fundamental rights and civil liberties.

Harris (2020) notes that data processing for the exercise of public authority may raise questions in terms of the precepts that underpin the rule of law. This is due to the possibility of reducing transparency in the functioning of a given public policy, so transparency takes on a crucial role in enabling citizens as data subjects to comprehend the functioning of data processing activity used to implement public policies (HARRIS, 2020). In this respect, Harris emphasizes that the process of developing an impact assessment poses an opportunity to implement the principle of publicity, and its fulfillment unfolds into active and passive transparency measures for the public authority, and the principle of public participation (HARRIS, 2020).

On the public authority duty of publicizing data protection impact assessments, Harris (2020) states that their publication by default would add to transparency, and accountability, as far as it would enable civil society to exercise oversight and hold thorough public debates around these data processing operations, resulting in a more trusting relationship between the Public Administration and those administered.

As an example, there are successful cases in which data protection impact assessments were compiled by the public authority and their publication led to qualitative improvement for risks in certain data processing operations. Since June 2019, the Dutch government has engaged the services of Privacy Company to compile data protection impact assessments on certain Microsoft apps used in local universities and schools, such as Teams, OneDrive, SharePoint, and Azure AD, to identify risks to data subjects. Once compiled, these reports were publicized, explicitly showing which risks were identified, as well as these apps' weaknesses. This process subsequently led to negotiations between the Dutch government and Microsoft in which the company was asked to take measures to mitigate high-level risks to data subjects. The negotiations resulted in Microsoft's commitment to respond to demands that emerged from the personal data protection impact assessment and therefore added more protection for Dutch citizens directly affected by these risks (PRIVACY COMPANY, 2022).

b. Data Protection Impact Assessment: a necessary relationship between regulation–governance *ex ante* and *ex post*

This document has discussed the fact that impact assessments and, more specifically, DPIAs, fulfill the objective of enabling all data subjects involved and interested in data processing operations to understand and influence the decision-making process (BIONI *et al*, 2020). This means, according to Kloza (2014), that impact assessments are related to an aspect of procedural justice, since they are not just about obtaining fair results, but also ensuring that the route traveled to reach this result is fair too.

In this sense, Bioni *et al* (2020, p. 8) argues that, in addition to assisting the process of compliance with data protection legislation, impact assessments: "are tributary from that which is conventionally called information due process. This means ensuring not only that there are transparency measures, but also control over a decision that will affect public and individual freedoms".

Therefore, there needs to be a confluence between two regulatory types: ex-ante and ex-post regulation. The first, as pointed out in sections 5.1 and 5.2 of this document, is narrowly related to the very nature of data protection risk-taking and data protection impact assessment processes. In other words, it follows an anticipatory rationale that aims to assess the risks and benefits of implementing a particular personal data processing operation, especially by the public authorities. The ex-post regulation, on the other hand, should guide regulatory rationality after conducting an impact assessment, based on the conception that the DPIA is a living instrument and that it needs to be updated whenever there is any change in the activity of processing personal data. That is, the concretization of adverse effects and benefits throughout the data operation is a learning experience for the progressive sophistication of the risk management in question.

This need for overlapping between two regulatory models is shown based on realizing that impact assessments must be incorporated and reviewed throughout a given project's life cycle. Therefore, impact assessments must be compiled as soon as possible in order to influence the way in which processing – or, in the case of this document, public policy for data processing – will be designed, and monitor the entire evolutionary cycle of this operation so that its DPIA may be revisited if new risks are detected (KLOZA, 2014).

In this respect, considering the high risks to data subjects that were identified throughout chapters 3 and 4 of this policy paper - which arises from both the National Civil Identification system's information architecture and the use of the ICN Database to authenticate gov.br platform users - compiling data protection impact assessments become mandatory

for both processes. The obligation to conduct them highlights the DPIA as an important process to be developed by public authority processing agents.

Properly compiling – and oriented towards the principles related to procedural justice – data protection impact assessments will help in the process of guaranteeing data subjects' fundamental rights. As a result, a bridge may be built to reach social justice by developing a civil identification system in which data processing operations are more transparent and risks to data subjects are properly identified and mitigated. On this basis, the visibility-exclusion dilemma may be adequately addressed by prioritizing the inclusion of subjects that have historically been invisiblized and excluded from access to public services and basic public policies for the full exercise of citizenship.

6. Conclusions

6.1. Summary of risks arising from the ICN and use of the BDICN to authenticate citizens on gov.br

This document has consistently pointed to the fact that Brazil's National Civil Identification system has yet to be fully implemented, despite constant efforts made over recent years. Hence the ICN database is being used mostly in the context of gov.br, the platform which corresponds to the federal government's initiative to gather digital public services together in one single environment.

Based on this scenario, this report, supported by the dialectical relationship established by the visibility-exclusion dilemma, has sought to map risks to citizens - also identified as data subjects - shown by the ICN's information architecture and its relationship with the gov.br platform. These risks were divided into two categories: (i) risks related to ICN's information architecture and governance arrangements - or risks of abusive use of personal data; and (ii) risks of excluding citizens arising from the phenomenon of platforming public services and using BDICN to authenticate gov.br platform users.

As for the first category, the risks identified are related to the visibility dimension posed by the aforementioned dilemma and arise from the information architecture itself and the ICN governance arrangements established by the ICN Law's goal of creating a single centralized database consisting of several other public databases, such as the Electoral Court system's biometric database. These risks have been further detailed in chapter 3 of this document and are summarized in the following table:

Group 1: risk of abuse when processing personal data, related to ICN's information and governance architecture		
Source of risk identified	Reason	Fundamental rights and civil liberties potentially violated by identified risks
Lack of plurality of views in the governance process for a complex public policy	A non-multi-sectoral composition of a governance body, such as ICN's Management Committee and the Federal Executive Chamber for Citizen Identification (CEFIC) – the latter established by	Potentially all of them - they cannot be delimited; ultimately governance choices will determine which rights and freedoms will be affected. In this respect, limiting society's participation

	Decree No. 10.900/2021 –may fail to reflect the plurality of views required for the proper governance process of a public policy as complex as ICN and gov.br	could affect the Brazilian State's democratic regime.
Secondary and/or shared uses of personal data stored in ICN's database, in contrast to the principle of purpose limitation (article 6, I, LGPD)	There is a risk of abusive secondary use of personal data in ICN policy, which is particularly visible in four aspects: **(i)** the BDICN was set up by conjoining databases from other public spheres, whose purposes are not necessarily compatible with ICN policy; **(ii)** Using BDICN to authenticate users on the gov.br platform, which could mean deviating from the original purpose of ICN's data processing activities; **(iii)** Use of BDICN to cross-reference citizens' data in order to verify compliance with requirements for access to social benefits; **(iv)** Possibility of the Executive and Legislative Powers accessing the BDICN without any procedure for verifying their purpose of access.	**(i)** Violation of information self-determination, considered as a development of the fundamental right to personal data protection stipulated in the Federal Constitution's art. 5, LXXIX. **(ii)** Violation of human dignity, established as one of the foundations of the Federative Republic of Brazil, pursuant to the Federal Constitution's art. 1, III. **(iii)** Violation of the principle of non-discrimination, established as one of the foundations of the Federative Republic of Brazil, pursuant to the Federal Constitution's art. 3, IV, and the dignity of the human person as defined its art. 1, III. **(iv)** Violation of information self-determination, considered as a development of the fundamental right to personal data protection stipulated in the Federal Constitution's art. 5, LXXIX.
Discriminatory treatment of citizens and authoritarian practices	In addition to centralized information architecture, the ICN Database holds a huge diversity of data, including biometric data, which may enhance: **(i)** surveillance practices by the State; **(ii)** the unlawful exclusion of citizens from social assistance benefits based on discriminatory data processing, as per LICN Article 11.	**(i)** Mass surveillance has a chilling effect by lowering citizen participation in public spaces for fear of being watched by government, thus threatening the freedom of expression and assembly assured by art. 5th, IV, IX and XVI[48]. **(ii)** Discriminatory treatment puts equality at risk, which is guaranteed by the constitution's article 5, heading, item I, XLI, which determines with punishment any

48 For more details, see Article 19 (2021).

		discriminatory practice harming an individual's fundamental rights and freedoms, as well as XLII, which defines racism as a crime, that is non-bailable and without a statutory period of limitation.
Violation of the data quality principle (article 6, V, LGPD)	According to the TSE there are some inconsistencies in the electoral biometric database: **(i)** In 2018, 9 million voters had a problem with immediate biometric identification during the elections. **(ii)** Since 2014, some 52,000 cases related to two or more identical biometrics have been identified.	**(i)** Impossibility of accessing public services via gov.br platform, access to public services is assured by the Constitution's art. 175. **(ii)** Difficulties when identifying voters to exercise the right to suffrage established by the Federal Constitution's art. 14.
Security incidents involving ICN Database	The BDICN holds (sensitive) biometric data of more than 110 million Brazilians, which amounts to large-scale data processing. A centralized information architecture becomes more likely to be targeted for severe security incidents since even a single episode could give access to a large amount and diversity of citizens' personal data, including sensitive data such as biometric data. In addition, security incidents involving biometric data reveal the even greater potential for harm, since these data are directly related to the data subject's body, so they cannot be altered.	Violation of human dignity established as one of the foundations of the Federative Republic of Brazil, according to the Federal Constitution's art. 1, III. From the United Nations High Commissioner for Human Rights report, August 2018 (A/HRC/39/29), "identity theft based on biometric data is extremely difficult to remediate and may severely affect an individual's rights."
Citizens' exercise of data subject rights stipulated by the LGPD	The gov.br platform, which uses the ICN Database to authenticate its users, as far as its interface and privacy policy are visible, does not have a direct and adequate communication channel enabling citizens to request confirmation of the existence of data processing, access to their processed data and rectification of incorrect or outdated data.	Violation of information self-determination, in its aspect of developing the fundamental right to personal data protection per the Federal Constitution's art. 5, LXXIX.

In turn, the second category of mapped risks deals with those that emerge from using the BDICN to authenticate users on the gov.br platform to authorize citizens' access to

public services, and the structuring of the platform per se. Therefore, these risks – which were detailed in chapter 4 of this document – relate directly to the second aspect of the abovementioned dilemma, namely citizens being excluded from access to public policies and services. These may be schematically visualized in the following table:

Group 2: risk of excluding citizens from access to public services		
Source of risk identified	Reason	Fundamental rights and civil liberties that may be violated by the identified risks
Exclusion of access to public services for people who do not have any identity document	The gov.br platform uses BDICN to authenticate its users through a unique login, so to access digitized public services via gov.br, citizens must have their personal data cataloged in BDICN. To do so, they must have an identification document, which depends on a birth certificate to be issued - Brazil's "foundational document". Therefore, those not having this document are excluded from gov.br: this segment of the population is more numerous in the North and Northeast regions.	Exclusion of access to public rights and policies, such as social rights related to work and social security, for example the impossibility of issuing an Employment and Social Security Card (CTPS) and of providing evidence of life for the National Insurance Institute (INSS), both constitutionally established as social rights by art. 6.
Exclusion of access to public services for people whose identity documents are in some way inadequate	The inadequacy of identity documents for trans people has the potential to exclude this population from accessing gov.br and, consequently, from public services accessed through the platform. This risk stems from the inexistence, in the ICN and in the gov.br portal, of a field for the inclusion of social name, so a person cannot be identified by the name they use and by which they are socially recognized.	Exclusion of access to public rights and policies, such as social rights related to work and social security, being unable to get an Employment and Social Security Card (CTPS) issued and provide evidence of life for the National Insurance Institute (INSS), both of which are constitutionally established as social rights in art. 6.
Exclusion from access to public services for hyper-vulnerable subjects such as children, adolescents, seniors, and people with disabilities	**Children and adolescents:** **(i)** Due to their age, their data have not been entered into the databases used (from the Electoral Courts and State Traffic Departments - DETRANs).	**(i)** Exercising rights and enjoying digital public policies and services being difficult or infeasible, thus violating the Child and Adolescent Statute's art. 3.

	(ii) Since they do not possess biometric data registered with the BDICN, they may be unable to reach the maximum level of authentication, which is granted by biometric validation of the Electoral Court system data and data validation of digital certificates. **Seniors:** **(i)** Exclusion is associated with difficulties in using computers, cell phones, and the Internet resulting from illiteracy and functional illiteracy. **People with disabilities:** **(i)** The gov.br platform's authentication procedures are not accessible or inclusive for people with disabilities.	**(ii)** Impossibility of exercising social rights related to the elderly, such as access to social security, established by the Federal Constitution's art. 6. **(iii)** Difficulty or impossibility of accessing digital public services, due to lack of accessibility, violating art. 4 of the Statute of Persons with Disabilities.
People being excluded from access to public services due to the absence or poor quality of Internet access	In this instance, the exclusion is brought on by the fact that citizens are unable to use the gov.br platform because they have partial or no Internet access at all. Recent data show that the absence of full Internet access is more often found among people from the most vulnerable social classes, who may even stop accessing public services due to a lack of connection.	Being excluded from access to public rights and policies such as social rights related to employment and social security or being unable to get an Employment and Social Security Card (CTPS) issued or provide evidence of life required by the National Social Insurance Institute (INSS), breaches constitutionally established social rights under art. 6.

6.2. Risks and rights: the obligation of compiling and publishing Personal Data Protection Impact Assessment

As noted above, the data protection impact assessment is an important accountability tool established by the General Data Protection Law, whose conduction is linked to the notion of data subjects' risks arising from a given data processing activity.

Although Brazil's legal system does not yet have a standardized procedure for compiling DPIAs, their use internationally is driven by the existence of a high level of risk for

data subjects' fundamental rights and civil liberties. The European Union's General Data Protection Regulation is pointing in the same direction too.

In the Brazilian context, DPIA regulations are being drafted by the National Data Protection Authority and are expected to be on the Authority's Regulatory Agenda for 2021-2022. However, pointers from the ANPD as to what the legal system considers high-risk data processing activity have already been detected - cases in which a data protection impact assessment must be compiled. As noted in section 5.3 of this document, the resolution published by the ANPD on the application of the LGPD to small-scale processing agents establishes a series of criteria, divided between general and specific criteria; the ICN and its use on gov.br fulfill criteria for large-scale data processing and use of sensitive personal and seniors' data. This is already sufficient to be rated high-risk processing, in which case compiling a DPIA is mandatory.

In other words, considering this normative-regulatory scenario and the public policies analyzed in this policy paper – namely, National Civil Identification and use of the ICN database to authenticate gov.br platform users – one concludes that data processing activities constituting these public policies meet the criteria for high-risk ratings since they basically involve large-scale data processing and use of sensitive personal data.

Therefore, based on a systematic interpretation of Brazilian law in terms of regulations and guidelines classifying data processing activities' high level of risk for data subjects, and when a DPIA is recommended, this assessment is mandatory both for implementing National Civil Identification and for the ICN database being used to authenticate gov.br platform users. The purpose of this obligation is to assist in the process of tackling the visibility-exclusion dilemma imposed by the implementation of a centralized digital identity system, to mitigate its risks.

In addition to the obligation of issuing a DPIA, the process of compiling this assessment must be based on sound scientific methodology as applied to risk analysis. Furthermore, the assessment must consider at least the risks identified in chapters 3 and 4 of this document, which have been summarized in tables, since they relate to potential violations of fundamental rights to access public services and civil identification, which constitutes one of the cornerstones of the full exercise of citizenship; in addition to the minimum content established by article 5-XVII and article 38 sole paragraph, and other risks that may not have been identified by this policy paper.

Moreover, chapter 5 of this document noted that a DPIA - although contributing to a given organization's process of compliance with personal data protection legislation - is

not a compliance document, since the data subject is its center of gravity. In other words, the impact assessment objective is to guarantee data subjects' fundamental rights and civil liberties. In addition, a DPIA must be a living document to be constantly revisited and updated whenever there are changes in personal data processing activities that prompt the emergence of new risks for data subjects.

The DPIA thus emerges as a powerful accountability tool. As such, publicizing a DPIA is an essential element to reaching objectives such as enabling society's effective participation.

The General Data Protection Law does not determine which situations would culminate in the DPIA being publicized. However, one may verify that, according to the LGPD's article 32, publicizing involves specific aspects when the assessment is based on the government's processing of personal data. So, a systematic interpretation of the LGPD and Public Administration constitutional principles - especially the principle of publicity - leads to the conclusion that there is a duty to publicize DPIAs on the part of the public authority, as shown in this document's chapter 5, subsection 5.3a.

The government publicizing DPIAs by default may well ensure more transparency and accountability for public data processing agents. Furthermore, it enables society to deepen its participation in public policymaking processes that involve large-scale personal data processing, as well as the possibility of public policies being monitored by civil society - which is directly affected by these policies.

Hence our concluding that conducting data protection impact assessments for the implementation of National Civil Identification and for the use of the ICN database to authenticate gov.br platform users is a crucial first step towards public data processing policies becoming transparent, accountable and able to show that the right measures have been taken to mitigate risk for data subjects. To do so, these documents must be publicized, given their relevant public interest.

A properly compiled and publicized personal data protection impact assessment should be seen as an ally to deal with the visibility-exclusion dilemma. Identifying and mitigating the risks of a unified digital identity system, as proposed by the ICN, and the use of its database on the gov.br platform, are crucial ways of finding the correct balance between the risks and benefits of these public policies, which are crucial for the exercise of citizenship in Brazil.

References

AGÊNCIA BRASIL.**Governo atinge marca de 1,5 mil serviços digitalizados em 34 meses**. 04 nov. 2021. Available at: <https://agenciabrasil.ebc.com.br/geral/noticia/2021-11/governo-atinge-marca-de-15-mil-servicos-digitalizados-em-34-meses>. Accessed May 11, 2022.

AGÊNCIA NACIONAL DE TELECOMUNICAÇÕES. **Resolução nº 650, de 16 de março de 2015**. 01 jun. 2021. Available at: <https://informacoes.anatel.gov.br/legislacao/resolucoes/2015/790-resolucao-650>. Accessed May 12, 2022.

ALMEIDA, Virgílio; GETSCHKO, Demi; AFONSO, Carlos A. The Origin and Evolution of Multistakeholder Models. IEEE Internet Computing, n.19, v. 1, 74–79, 2015. Available at: <https://www.computer.org/csdl/magazine/ic/2015/01/mic2015010074/13rRUNvya5I>. Accessed May 13, 2022.

AMNESTY INTERNATIONAL. Xenophobic machines: Discrimination through unregulated use of algorithms in the Dutch childcare benefits scandal, 2021. Available at: <https://www.amnesty.org/en/documents/eur35/4686/2021/en/>. Accessed May 17, 2022.

ARTICLE 19. When bodies become data: Biometric technologies and free expression, 2021. Available at: <https://www.article19.org/wp-content/uploads/2021/05/Biometric-Report-P3-min.pdf>. Accessed May 18, 2022.

ARTICLE 29 DATA PROTECTION WORKING PARTY - WP 29. Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. [s.l.], 2014. Available at: <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp217_en.pdf>. Accessed May 18, 2022.

ANDRADE, Eduardo Goulart *et al*. Dados Virais: Legado da COVID-19 nas aquisições de tecnologias pelo Poder Público. Associação Data Privacy Brasil de Pesquisa, 2021. Available at: <https://drive.google.com/file/d/1-PmjyYubF65W_8LuOiYR2pwFQiRWEyZ3/view>. Accessed May 13, 2022.

ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA. Accountability e Identidade Civil Digital, s.d a. Página projeto Accountability e Identidade Civil Digital. Available at: <https://www.dataprivacybr.org/projeto/accountability-e-identidade-civil-digital/>. Accessed May 09, 2022.

ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA. Apresentação na Turing trustworthy digital identity conference, s.d. b Available at: <https://www.dataprivacybr.org/documentos/apresentacao-na-turing-trustworthy-digital-identity-conference/>. Accessed May 09, 2022.

ASSOCIAÇÃO DATA PRIVACY BRASIL DE PESQUISA. Oficina sobre Relatório de Impacto à Proteção de Dados e identidade civil digital, s.d c. Available at: <https://www.dataprivacybr.org/documentos/oficina-sobre-relatorio-de-impacto-a-protecao-de-dados-e-identidade-civil-digital/>. Accessed May 18, 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD. Portaria nº 11, de 27 de janeiro de 2021. **Torna pública a agenda regulatória para o biênio 2021-2022**. Brasília, 2021 Available at: <https://www.in.gov.br/en/web/dou/-/portaria-n-11-de-27-de-janeiro-de-2021-301143313>. Accessed May 09, 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD. Resolução CD/ANPD nº 2, de 27 de janeiro de 2022. Aprova o Regulamento de aplicação da Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), para agentes de tratamento de pequeno porte. Brasília, 2022. Available at: <https://in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-2-de-27-de-janeiro-de-2022-376562019?utm_source=google-search&utm_medium=cpc&utm_campaign=totvs_conversao_sql&utm_term[0]=s-institucional_Totvs&utm_term[1]=totvs&utm_content=eta-v4>. Accessed May 09, 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD. Guia Orientativo: Tratamento de dados pelo Poder Público. Brasília, jan. 2022. Available at: <https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/guia-poder-publico-anpd-versao-final.pdf>. Accessed May 18, 2022.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS - ANPD. Conselho Nacional de Proteção de Dados Pessoais e da Privacidade. 10 mai 2022. Available at: <https://www.gov.br/anpd/pt-br/composicao-1/conselho-nacional-de-protecao-de-dados-pessoais-e-privacidade-cnpd>. Accessed May 12, 2022.

BANCO MUNDIAL. ID4D: About us, 2022. Available at: <https://id4d.worldbank.org/about-us>. Accessed May 10, 2022.

BANCO MUNDIAL. ID4D: Country Engagement, 2022. Disponível em <https://id4d.worldbank.org/country-engagement>. Accessed May 10, 2022.

BBC. Aadhaar: 'Leak' in world's biggest database worries Indians. 5 de Janeiro de 2018. Available at: <https://www.bbc.com/news/world-asia-india-42575443>. Accessed May 16, 2022.

BIONI, Bruno Ricardo; LUCIANO, Maria. O princípio da precaução na regulação de inteligência artificial: seriam as leis de proteção de dados o seu portal de entrada? *In*: FRAZÃO, Ana; MULHOLLAND, Caitlin (orgs.). Inteligência Artificial e Direito: ética, regulação e responsabilidade. São Paulo: Revistas dos Tribunais, 2019.

BIONI, Bruno; RIELLI, Mariana. Salvaguardas regulatórias: entre princípio da precaução e relatórios de impacto. *In*: BIONI, Bruno; ZANATTA, Rafael; RIELLI, Mariana (orgs.). Data Privacy Br: Contribuição à consulta pública da Estratégia Brasileira de Inteligência Artificial. São Paulo: Reticências Creative Design Studio, 2020. Available at: <https://www.dataprivacybr.org/wp-content/uploads/2020/06/E-BOOK-CONTRIBUIÇÃO-DPBR-INTELIGÊNCIA-ARTIFICIAL-FINAL.pdf>. Accessed May 10, 2022.

BIONI, Bruno *et al.* Proteção de dados no campo penal e de segurança pública: nota técnica sobre o Anteprojeto de Lei de Proteção de Dados para segurança pública e investigação criminal. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2020. Available at: <https://www.dataprivacybr.org/wp-content/uploads/2020/12/NOTA-TÉCNICA-PROTEÇÃO-DE-DADOS-NO-CAMPO-PENAL-E-DE-SEGURANÇA-PÚBLICA-VF-31.11.2020.pdf>. Accessed May 11, 2022.

BIONI, Bruno. Proteção de dados pessoais: a função e os limites do consentimento. 3 ed. Rio de Janeiro: Forense, 2021.

BOCCHINI, Bruno. Pesquisa mostra exclusão de idosos do mundo digital e da escrita. Agência Brasil. São Paulo, 21 ago. 2020. Available at: <https://agenciabrasil.ebc.com.br/geral/noticia/2020-08/pesquisa-mostra-exclusao-de-idosos-do-mundo-digital-e-da-escrita>. Accessed May 17, 2022.

BRASIL. Lei nº 6.015, de 31 de dezembro de 1973. Dispõe sobre os registros públicos, e dá outras providências.. Brasília, 1973. Available at: <http://www.planalto.gov.br/ccivil_03/leis/l6015compilada.htm>. Accessed May 18, 2022.

BRASIL. Lei nº 7.116, de 29 de agosto de 1983. Assegura validade nacional as Carteiras de Identidade regula sua expedição e dá outras providências. Brasília, 1983. Available at: <http://www.planalto.gov.br/ccivil_03/leis/1980-1988/l7116.htm>. Accessed May 18, 2022.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, 1990. Available at: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>. Accessed May 11, 2022.

BRASIL. Lei nº 10.741, de 1º de outubro de 2003. Dispõe sobre o Estatuto do Idoso e dá outras providências. Brasília, 2003. Available at: <http://www.planalto.gov.br/ccivil_03/leis/2003/l10.741.htm>. Accessed May 11, 2022.

BRASIL. Lei nº 13.146, de 6 de julho de 2015. Estatuto da Pessoa com Deficiência. Brasília, 2015. Available at: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13146.htm>. Accessed May 11, 2022.

BRASIL. Lei 13.444, de 11 de maio de 2017. Dispõe sobre a Identificação Civil Nacional (ICN). Brasília, 2017. Available at: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/l13444.htm>. Accessed May 17, 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais**. Brasília, 2018. Available at: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Accessed May 09, 2022.

BRASIL. Lei nº 13.848, de 25 de junho de 2019. Lei das Agências Reguladoras. Brasília, 2019. Available at: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13848.htm>. Accessed May 18, 2022.

BRASIL. Decreto nº 10.900, de 17 de dezembro de 2021. Dispõe sobre o Serviço de Identificação do Cidadão e a governança da identificação das pessoas naturais no âmbito da administração pública federal direta, autárquica e fundacional, e altera o Decreto nº 8.936, de 19 de dezembro de 2016, o Decreto nº 10.543, de 13 de novembro de 2020, e o Decreto nº 9.278, de 5 de fevereiro de 2018. Brasília, 2021a. Available at: <https://www.in.gov.br/en/web/dou/-/decreto-n-10.900-de-17-de-dezembro-de-2021-368282514>. Accessed May 16, 2022.

BRASIL. Acordo de Cooperação Técnica que firmam entre si a Secretaria-Geral da Presidência da República, o Ministério da Economia e o Tribunal Superior Eleitoral, objetivando a cooperação para implementação da Identificação Civil Nacional. Brasília, 15 mar. 2021b. Available at: <https://www.tse.jus.br/imprensa/noticias-tse/arquivos/act-identificacao-civil-nacional/rybena_pdf?file=https://www.tse.jus.br/imprensa/noticias-tse/arquivos/act-identificacao-civil-nacional/at_download/file>. Accessed May 18, 2022.

BRASIL. Lei nº 14.129, de 29 de março de 2021. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública e altera a Lei nº 7.116, de 29 de agosto de 1983, a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), a Lei nº 12.682, de 9 de julho de 2012, e a Lei nº 13.460, de 26 de junho de 2017. Brasília, 2021c. Available at: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm>. Accessed May 17, 2022.

BRASIL. Câmara dos Deputados. Projeto de Lei nº 3.228, de 20 de set. 2021. Altera a Lei nº 13.444, de 11 de maio de 2017, que dispõe sobre a Identificação Civil Nacional - ICN. Brasília: Câmara dos Deputados, 2021. Available at: <https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=2076542>. Accessed May 17, 2022.

BRASIL. Portaria nº 667, de 9 de fevereiro de 2022. Agenda Legislativa Prioritária do Governo Federal para o ano de 2022. Brasília, 2022. Available at: <https://www.in.gov.br/en/web/dou/-/portaria-n-667-de-9-de-fevereiro-de-2022-379226707>. Accessed May 17, 2022.

BRODERSEN, Juan; BLANCO, Pablo Javier. Un cibercriminal que asegura haber robado datos de 45 millones de DNI difundió fotos de políticos, periodistas y famosos en Twitter. Clarín, Buenos Aires, 13 de Outubro de 2021. Available at: <https://www.clarin.com/tecnologia/ciberdelincuente-asegura-robado-datos-45-millones-dni-difundio-fotos-politicos-periodistas-famosos-twitter_0_QBD5xKDNM.html>. Accessed May 16, 2022.

BRODERSEN, Juan; BLANCO, Pablo Javier. "Quizás publique los datos personales de 1 o 2 millones de personas", dijo el usuario que filtró fotos de los DNI de políticos, famosos y periodistas. Clarín, Buenos Aires, 19 de Outubro de 2021. Available at: <https://www.clarin.com/tecnologia/-publique-datos-personales-1-2-millones-personas-dijo-usuario-filtro-fotos-dni-politicos-famosos-periodistas_0_SgsEoUeQj.html?utm_term=Autofeed&utm_medium=Social&utm_source=Twitter#Echobox=1634683887>. Accessed May 16, 2022.

CÂMARA DOS DEPUTADOS. Pandemia acelera o uso de serviços públicos digitais: ao todo, há 4.699 serviços por meio do portal do governo federal, 2021. Available at: <https://www.camara.leg.br/noticias/809660-pandemia-acelera-o-uso-de-servicos-publicos-digitais/>. Accessed May 10, 2022.

CARVALHO FILHO, José dos Santos. Manual de Direito Administrativo. 34. ed. São Paulo: Atlas, 2020.

CARIBOU DIGITAL. Identification, identity, and sexuality in Brazil, 2020. Available at: <https://medium.com/caribou-digital/identification-identity-and-sexuality-in-brazil-da5464a634d2>. Accessed May 11, 2022.

CENTRO DE ESTUDOS DE CULTURA CONTEMPOR NEA - CEDEC. Mapeamento das pessoas trans no município de São Paulo: relatório de pesquisa. São Paulo, 2021. Available at: <https://www.prefeitura.sp.gov.br/cidade/secretarias/upload/direitos_humanos/LGBT/AnexoB_Relatorio_Final_Mapeamento_Pessoas_Trans_Fase1.pdf>. Accessed May 17, 2022.

CENTRO REGIONAL DE ESTUDOS PARA O DESENVOLVIMENTO DA SOCIEDADE DA INFORMAÇÃO (CETIC.br). Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros : TIC Domicílios 2020: edição COVID-19: metodologia adaptada, São Paulo: Comitê Gestor da Internet, 2021. Available at: <https://cetic.br/media/docs/publicacoes/2/20211124201233/tic_domicilios_2020_livro_eletronico.pdf>. Accessed May 11, 2022.

CLARKE, Roger. Privacy impact assessment: its origins and development. Computer Law & Security, [s.l], n. 25, 2009. Available at: <https://openresearch-repository.anu.edu.au/bitstream/1885/53679/2/01_Clarke_Privacy_impact_assessment%3A_Its_2009.pdf>. Accessed May 10, 2022.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Regimento Interno do Comitê Gestor da Internet no Brasil**, s.d. Available at: <https://www.cgi.br/pagina/regimento-interno-do-comite-gestor-da-internet-no-brasil/308/>. Accessed May 12, 2022.

CONSELHO NACIONAL DE JUSTIÇA - CNJ. Provimento nº 46, de 16 de julho de 2015. Revoga o Provimento 38 de 25/07/2014 e dispõe sobre a Central de Informações de Registro Civil das Pessoas Naturais - CRC. Brasília, 2015. Available at: <https://atos.cnj.jus.br/files//provimento/provimento_46_16062015_16032018111049.pdf>. Accessed May 18, 2022.

DAHL-JØRGENSEN, Tangni Cunningham, PARMIGGIANI, Elena. Platformization of the public sector: Assessing the space of possibility for participation. Proceedings of the 16th Participatory Design Conference - Participation(s) Otherwise - Volume 2, 2020. Available at: <https://dl.acm.org/doi/10.1145/3384772.3385154>. Accessed May 13, 2022.

DAMASCENO, Victoria. Cadastro do SUS e sistema que emite certificado de vacina impedem uso de nome social. Folha de São Paulo. São Paulo, 28 jan. 2022. Available at: <https://www1.folha.uol.com.br/equilibrioesaude/2022/01/cadastro-do-sus-e-sistema-que-emite-certificado-de-vacina-impedem-uso-de-nome-social.shtml?utm_source=twitter&utm_medium=social&utm_campaign=twfolha>. Accessed May 17, 2022.

DANTCHEVA, Antitza; ELIA, Petros; ROSS, Arun. What Else Does Your Biometric Data Reveal? A Survey on Soft Biometrics. IEEE Transactions on Information Forensics and Security, vol. 11, n. 3, 2016. Available at: <https://ieeexplore.ieee.org/document/7273870>. Accessed May 18, 2022.

DATA PRIVACY BRASIL. Oficina sobre Relatório de Impacto à Proteção de Dados para o Poder Público. Youtube, 13 de jan. de 2022. Available at: <https://www.youtube.com/watch?v=sLBc1nLTcFA&t=2758s>.

DIJCK, José Van; POELL, Thomas; DE WAAL, Martijn. **The Platform Society**. Nova Iorque: Oxford University Press, 2018.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais: fundamentos da Lei Geral de Proteção de Dados. 2. ed., São Paulo: Thomson Reuters Brasil, 2019.

DONEDA, Danilo; KANASHIRO, Marta. A transformação da identificação e a construção de bancos de dados: o caso do documento único no Brasil. *In*: BRUNO, Fernanda; KANASHIRO, Marta; FIRMINO, Rodrigo (orgs.). Vigilância e visibilidade: espaço, tecnologia e identificação, Porto Alegre: Sulina, 2010, p. 272-296.

ESCÓSSIA, Fernanda Melo da. Invisíveis: Uma etnografia sobre identidade, direitos e cidadania nas trajetórias de brasileiros sem documento. 2019. Tese (Doutorado) - Programa de Pós-Graduação em História, Política e Bens Culturais do Centro de Pesquisa e Documentação em História Contemporânea do Brasil, Fundação Getúlio Vargas, 2019. Available at: <https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/27459/Tese%20Fernanda%20da%20Escóssia.pdf?sequence=1&isAllowed=y>. Accessed May 17, 2022.

EUBANKS, Virginia. Automating Inequality: How High-Tech Tools Profile, Police and Punish the Poor. St Martin's Press: 2018.

FAULKNER-GURSTEIN, Rachel; WYATT, David. Platform NHS: Reconfiguring a Public Service in the Age of Digital Capitalism. **Science, Technology, & Human Values**, p. 01-21, 22 nov. 2021. Available at: <https://journals.sagepub.com/doi/10.1177/01622439211055697>. Accessed May 12, 2022.

GARROTE, Marina *et al.* A ICN e o futuro da identidade civil (digital) no Brasil, Jota, [s.l.], 04 out 2021a. Available at: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/a-icn-e-o-futuro-da-identidade-civil-digital-no-brasil-04102021>. Accessed May 16, 2022.

GARROTE, Marina *et al.* ANPD na regulamentação do Relatório de Impacto à Proteção de Dados Pessoais, Jota, [s.l.], 13 jun 2021b. Available at: <https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/anpd-relatorio-impacto-protecao-dados-pessoais-13072021>. Accessed May 09, 2022

GELB, Alan.; CLARK, Julia. Identification for Development: The Biometrics Revolution. **SSRN Electronic Journal**, 2013.

GELLERT, Raphaël. Data protection: a risk regulation? Between the risk management of everything and the precautionary alternative. *International Data Privacy Law*, v. 5, n. 1, 2015 p. 3–19. Available at: <https://doi.org/10.1093/idpl/ipu035>. Accessed May 11, 2022.

GELLERT, Raphaël. We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection, European Data Protection Law Review, n. 4, v. 2, 2016. Available at: <https://edpl.lexxion.eu/article/edpl/2016/4/7>. Accessed May 11, 2022.

GOMES, Maria Cecília O. Relatório de impacto à proteção de dados pessoais. Revista do Advogado-AASP, n. 144, 2019. Available at: <https://www.academia.edu/41160034/Relatório_de_Impacto_a_Proteção_de_Dados_Pessoais_uma_breve_análise_da_sua_definição_e_papel_na_LGPD>. Accessed May 19, 2022.

GOMES, Maria Cecília O. Entre o método e a complexidade: compreendendo a noção de risco na LGPD. In Temas atuais de proteção de dados. PALHARES, Felipe (Coord.). São Paulo: Thomson Reuters Brasil, 2020, pp 245-271.

GOVERNO FEDERAL. Gov.br - Portal Único do Governo, s.d. Available at: <https://www.gov.br/sobre/> Accessed May 12, 2022.

GOVERNO FEDERAL. **Acordo de Cooperação agilizará a implementação da Identidade Digital**. 16 mai. 2021. Available at: <https://www.gov.br/casacivil/pt-br/assuntos/noticias/2021/marco/acordo-de-cooperacao-agilizara-a-implementacao-da-identidade-digital-1> Accessed May 12, 2022.

GOVERNO FEDERAL. Digitalização de serviços públicos já atinge mais de 100 municípios, entre eles São Paulo. 19 abr. 2022a. Available at: <https://www.gov.br/economia/pt-br/assuntos/noticias/2022/abril/digitalizacao-de-servicos-publicos-ja-atinge-mais-de-100-municipios-entre-eles-sao-paulo>. Accessed May 17, 2022.

GOVERNO FEDERAL. Fevereiro registra aumento de usuários na plataforma GOV.BR. 04 mai. 2022b. Available at: <https://www.gov.br/secretariageral/pt-br/noticias/2022/marco/fevereiro-registra-aumento-de-usuarios-na-plataforma-gov.br>. Accessed May 19, 2022.

GOVERNO FEDERAL. gov.br atinge 130 milhões de usuários. 06 jun. 2022c. Available at: <https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2022/06/gov-br-atinge-130-milhoes-de-usuarios>. Accessed June 07, 2022.

GRUPO DE PESQUISA EM POLÍTICAS PÚBLICAS PARA O ACESSO À INFORMAÇÃO – GPOPAI. Contribuições à Consulta Pública do Anteprojeto de Lei/APL de Proteção de Dados Pessoais. São Paulo: 02 de julho de 2015. Available at: <https://brunobioni.com.br/wp-content/uploads/2019/04/Contribuicao-GPoPAI-Dados-Pessoais_Diagramada.pdf>. Accessed May 23, 2022.

GRUPO DE TRABALHO DO ARTIGO 29 PARA PROTEÇÃO DE DADOS. Orientações relativas à Avaliação de Impacto sobre a Proteção de Dados (AIPD) e que determinam se o tratamento é "suscetível de resultar num elevado risco" para efeitos do Regulamento (UE) 2016/679, 2017. Available at: <https://ec.europa.eu/newsroom/article29/items/611236/en>. Accessed May 10, 2022.

HARRIS, Swee Leng. Data Protection Impact Assessments as rule of law governance mechanisms. Data & Policy. 2020. vol. 2,. Available at: <https://doi.org/10.1017/dap.2020.3>. Accessed May 18, 2022.

IGO, Sarah Elizabeth. **The known citizen : a history of privacy in modern America**. Cambridge, Massachusetts : Harvard University Press, 2018.

INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR - IDEC; INSTITUTO LOCOMOTIVA. Barreiras e limitações no acesso à internet e hábitos de uso e navegação na rede nas classes C, D e E, 2021. Available at: <https://idec.org.br/sites/default/files/pesquisa_locomotiva_relatorio.pdf>. Accessed May 11, 2022.

INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR - IDEC. Vazamentos de dados de saúde coloca consumidor em risco; veja o que fazer. 02 de Dezembro de 2020. Available at: <https://idec.org.br/noticia/vazamentos-de-dados-de-saude-coloca-consumidor-em-risco-veja-o-que-fazer>. Accessed May 16, 2022.

INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR - IDEC. Acesso à Internet na Região Norte do Brasil. Instituto Brasileiro de Defesa do Consumidor e Derechos Digitales. Mar. 2022. Available at: <https://idec.org.br/pesquisas-acesso-internet>. Accessed May 18, 2022.

INSTITUTO BRASILEIRO DE GEOGRAFIA E ESTATÍSTICA - IBGE. Pesquisa Estatísticas do Registro Civil: Nota técnica 01/2020 - Esclarecimentos sobre o Sub-Registro de Nascimentos, 2020. Available at: <https://biblioteca.ibge.gov.br/visualizacao/periodicos/3099/rc_sev_esn_2018.pdf>. Accessed May 17, 2022.

JUSTIÇA ELEITORAL. Biometria. [s.l.], s.d. Available at: <https://www.justicaeleitoral.jus.br/biometria/>. Accessed May 18, 2022.

KANASHIRO, Marta Mourão; DONEDA, Danilo. The new Brazilian identification system: Unique features of a general transformation. **Surveillance & Society**, v.10, n.1, p.18–27, 18 jul. 2012. Available at: <https://doi.org/10.24908/ss.v10i1.4272>. Accessed May 11, 2022.

KANG, Margareth; DONEDA, Danilo; SANTOS, Maike Wille. Políticas de identidade na era digital e o Registro Civil Nacional. **Em Debate**, Belo Horizonte, v. 8, n.6, p. 41-64, agosto 2016. Available at: <http://opiniaopublica.ufmg.br/site/files/artigo/4-Margareth-Kang.pdf>. Accessed May 11, 2022.

KANG, Margareth; LUCIANO, Maria; SANTOS, Maike Wille. Relatório das audiências públicas. In: Análise técnica elaborada pelo Projeto Privacidade Brasil: PLC nº 19/2017 – Identidade Civil Nacional. 2017.

KANG, Margareth; LUCIANO, Maria . Nota técnica. In: Análise técnica elaborada pelo Projeto Privacidade Brasil: PLC nº 19/2017 – Identidade Civil Nacional.

KEANE, Jonathan. Facial Recognition Apps Are Leaving Blind People Behind. Vice, [s.l], 22 mar. 2016. Available at: <https://www.vice.com/en/article/ezpzzp/facial-recognition-apps-are-leaving-blind-people-behind>. Accessed May 17, 2022.

KLOZA, Dariusz. Privacy Impact Assessments as a Means to Achieve the Objectives of Procedural Justice. Jusletter IT. Die Zeitschrift für IT und Recht, 2014. Available at: <https://researchportal.vub.be/en/publications/privacy-impact-assessments-as-a-means-to-achieve-the-objectives-o>. Accessed May 11, 2022.

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

KONDER, Carlos Nelson. O tratamento de dados sensíveis à luz da Lei 13.709/2018. *In*: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Org.). Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Thomson Reuters Brasil, 2019, p. 445-463.

LIMA, Maria Cristina Oliveira de. "Por causa de um papel eu não podia voltar pra casa com meu bebê". Revista Piauí, 22 fev. 2022. Available at: <https://piaui.folha.uol.com.br/por-causa-de-um-papel-eu-nao-podia-voltar-pra-casa-com-meu-bebe/>. Accessed May 18, 2022.

LISTER, Charles. Privacy and large-scale personal data systems. **The Personnel and Guidance Journal**, v. 49, n.3, p. 207–211, nov. 1970. Available at: <https://doi.org/10.1002/j.2164-4918.1970.tb03433.x>. Accessed May 16, 2022.

LOBO, Ana Paula. Serpro leva contrato de R$ 72 milhões para fazer a identificação civil nacional. Convergência Digital, 10 jan. 2022. Available at: <https://www.convergenciadigital.com.br/Governo/Serpro-leva-contrato-de-R%24-72-milhoes-para-fazer-a-identificacao-civil-nacional-59110.html>. Accessed May 17, 2022.

LOPEZ, Oscar. Reported murders, suicides of trans people soar in Brazil. Reuters, [s.l.], 8 de setembro de 2020. Available at: <https://www.reuters.com/article/us-brazil-lgbt-murders-trfn-idUSKBN25Z31O>. Accessed May 11, 2022.

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

MARÉCHAL, Nathalie. First They Came for the Poor: Surveillance of Welfare Recipients as an Uncontested Practice. **Media and Communication**, v. 3, n. 3, p. 56–67, 20 out. 2015. Available at: <https://www.cogitatiopress.com/mediaandcommunication/article/view/268>. Accessed May 10, 2022.

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 May 10, 2022.

MASIERO, Silvia.; SHAKTHI, S. Grappling with Aadhaar: Biometrics, Social Identity and the Indian State. **South Asia Multidisciplinary Academic Journal**, n. 23, 15 set. 2020. Available at: <https://journals.openedition.org/samaj/6279>. Accessed May 10, 2022.

MASIERO, Silvia; BAILUR, Savita. Digital identity for development: The quest for justice and a research agenda. **Information Technology for Development**, v. 27, n. 1, p. 1–12, 2 jan. 2021. Available at: <https://www.tandfonline.com/doi/full/10.1080/02681102.2021.1859669>. Accessed May 10, 2022.

MAYER-SCHÖNBERGER, Viktor. Generational Development of Data Protection in Europe. **Technology and Privacy: The New Landscape**. Cambridge, MA: The MIT Press. p.219-242.

MINISTÉRIO DA EDUCAÇÃO. Portaria nº 33 de 18 de janeiro de 2018. Brasília, 2018. Available at: <http://portal.mec.gov.br/index.php?option=com_docman&view=download&alias=72921-pcp014-17-pdf&-category_slug=setembro-2017-pdf&Itemid=30192>. Accessed May 17, 2022.

MINISTÉRIO DA ECONOMIA. Do Eletrônico ao Digital, 25 nov. 2019. Available at: <https://www.gov.br/governodigital/pt-br/estrategia-de-governanca-digital/do-eletronico-ao-digital>. Accessed May 23, 2022.

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA. Escritório de Projetos e Processos do RIC- EPP, s.d. Available at: <https://www.justica.gov.br/Acesso/governanca/escritorio-de-projetos-e-processos-do-ric-2013-epp>. Accessed May 11, 2022.

MINISTÉRIO DA SAÚDE. Portaria nº 1.820, de 13 de agosto de 2009. Brasília, 2009. Available at: <https://conselho.saude.gov.br/ultimas_noticias/2009/01_set_carta.pdf>. Accessed May 17, 2022.

MULHOLLAND, Caitlin; MATERA, Vinicius. O tratamento de dados pessoais pelo Poder Público. *In*: MULHOLLAND, Caitlin (org.). A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago, 2020, p. 217-236.

MURAKAMI WOOD, David.; FIRMINO, Rodrigo. Empowerment or repression? Opening up questions of identification and surveillance in Brazil through a case of 'identity fraud'. **Identity in the Information Society**, v. 2, n. 3, p. 297–317, dez. 2009. Available at: <http://link.springer.com/10.1007/s12394-010-0038-y>. Accessed May 10, 2022.

MURAKAWA, Fabio. 'Ninguém está totalmente preparado', diz Heleno sobre ataque hacker a sites do governo. Valor, Brasília, 13 de Dezembro de 2021. Available at: <https://valorinveste.globo.com/mercados/brasil-e-politica/noticia/2021/12/13/ninguem-esta-totalmente-preparado-diz-heleno-sobre-ataque-hacker-a-sites-do-governo.ghtml>. Accessed May 16, 2022.

NAÍSA, Letícia. Falha no sistema do Inep expõe dados de 5 milhões de estudantes; entenda. Uol, São Paulo, 10 de Setembro de 2021. Available at: <https://www.uol.com.br/tilt/noticias/redacao/2021/09/10/falha-no-sistema-do-inep-vaza-dados-de-5-milhoes-de-estudantes.htm>. Accessed May 16, 2022.

NATION. Judge orders State to regularise Huduma Namba roll out, 2021. Available at: <https://nation.africa/kenya/news/judge-orders-state-to-regularise-huduma-namba-roll-out-3582906>. Accessed May 10, 2022.

NISSENBAUM, Helen. Privacy in Context: Technology, Policy, and the Integrity of Social Life. California: Stanford University Press, 2010.

OCDE. **OECD Reviews of Digital Transformation: Going Digital in Brazil**. [s.l.] OCDE, 2020.

OPEN SOCIETY FOUNDATIONS. Nubian Rights Forum *et al.* v. the Honourable Attorney General of Kenya *et al.* ("NIIMS case"), 2022. Available at: <https://www.justiceinitiative.org/litigation/nubian-rights-forum-et-al-v-the-honourable-attorney-general-of-kenya-et-al-niims-case>. Accessed May 10, 2022.

POELL, Thomas.; NIEBORG, David.; VAN DIJCK, José. Platformisation. **Internet Policy Review**, v. 8, n. 4, 29 nov. 2019. Available at: <https://policyreview.info/node/1425>. Accessed May 12, 2022.

PRIVACY COMPANY. New DPIA for the Dutch government and universities on Microsoft Teams, OneDrive and SharePoint Online. 21 fev. 2022. Available at: <https://www.privacycompany.eu/blog-post-en/new-dpia-for-the-dutch-government-and-universities-on-microsoft-teams-onedrive-and-share-point-online>. Accessed May 19, 2022.

PUPO, Amanda. Nove milhões tiveram problemas ao usar biometria, revela TSE. Exame, 27 out. 2018. Available at: <https://exame.com/brasil/nove-milhoes-tiveram-problemas-ao-usar-biometria-revela-tse/>. Accessed May 18, 2022.

QUELLE, Claudia. Does the Risk-Based Approach to Data Protection Conflict with the Protection of Fundamental Rights on a Conceptual Level? Tilburg Law School Research Paper, 2015.

REPUBLIC OF KENYA IN THE HIGH COURT OF KENYA AT NAIROBI CONSTITUTIONAL & JUDICIAL REVIEW DIVISION CONSOLIDATED PETITIONS NO. 56, 58 & 59 OF 2019, 30 jan 2020. Available at: <https://www.khrc.or.ke/publications/214-judgement-on-niims-huduma-namba/file.html>. Accessed May 16, 2022.

ROUBICEK, Marcelo. Desigualdade de gênero e raça: o perfil da pobreza na crise. Nexo, 25 abr. 2021. Available at: <https://www.nexojornal.com.br/expresso/2021/04/25/Desigualdade-de-gênero-e-raça-o-perfil-da-pobreza-na-crise>. Accessed May 17, 2022.

SAWHNEY, Ria Singh.; CHIMA, Raman Jit Singh.; AGGARWAL.; Naman M. **Busting the dangerous myths of Big ID Programs: cautionary lessons from India**. Access Now Publication, 2021.

SILVA, Priscila Regina. Os direitos dos titulares de dados. *In*: MULHOLLAND, Caitlin (org.). A LGPD e o novo marco normativo no Brasil. Porto Alegre: Arquipélago, 2020, p. 195-2015.

SIMITIS, Spiros. (1987). Reviewing Privacy In An Information Society. University Of Pennsylvania Law Review, v. 135, n. 3, 1987. Available at: <https://doi.org/10.2307/3312079>. Accessed May 17, 2022.

SOLANO, Joan Lopez *et al.* Digital disruption or crisis capitalism? Technology, power and the pandemic. Tilburg Institute for Law, Technology, and Society, 2022. Available at: <https://globaldatajustice.org/wp-content/uploads/2022/05/Global-Data-Justice-Digital-disruption-or-crisis-capitalism-03-2022.pdf>. Accessed May 25, 2022.

SPINA, Alessandro. A Regulatory Mariage de Figaro: risk regulation, data protection, and data ethics. European Journal of Risk Regulation , n. 8, v. 1, 88-94, 2017.

SUDRÉ, Lu. At least 124 trans people killed in Brazil in 2019: report. Brasil de Fato, São Paulo, 30 de Janeiro de 2020. Available at: <https://www.brasildefato.com.br/2020/01/30/at-least-124-trans-people-killed-in-brazil-in-2019-report>. Accessed May 11, 2022.

SUPREMO TRIBUNAL FEDERAL - STF. Decisão Mandado de Segurança 36.150 Distrito Federal, 17 dezembro 2021. Available at: <https://portal.stf.jus.br/processos/downloadPeca.asp?id=15349322719&ext=.pdf>. Accessed May 18, 2022.

TELESÍNTESE. Transformação digital do governo em desequilíbrio, diz TCU. 06 dez. 2021. Available at: <https://www.telesintese.com.br/transformacao-digital-do-governo-em-desequilibrio-diz-tcu/>. Accessed May 19, 2022.

THORSTENSEN, Vera; ZUCHIERI, Amanda Mitsue. Governo Digital no Brasil: o Quadro Institucional e Regulatório do País sob a Perspectiva da OCDE. Working Paper 529 – CCGI Nº 24 - FGV, 2020. Available at: <https://bibliotecadigital.fgv.br/dspace/bitstream/handle/10438/29177/TD%20529%20-%20CCGI_24.pdf?sequence=1&isAllowed=y>. Accessed May 11, 2022

TRIBUNAL DE CONTAS DA UNIÃO - TCU. **TCU avalia governança das estratégias de transformação digital da Administração Pública Federal**. 04 ago.2021. Available at: <https://portal.tcu.gov.br/imprensa/noticias/tcu-avalia-governanca-das-estrategias-de-transformacao-digital-da-administracao-publica-federal.htm>. Accessed May 12, 2022.

TRIBUNAL SUPERIOR ELEITORAL - TSE. Biometria. [s.l.], s.d. Available at: <https://www.tse.jus.br/eleitor/biometria>. Accessed May 18, 2022.

TRIBUNAL SUPERIOR ELEITORAL - TSE. Guia orientativo : aplicação da Lei geral de proteção de dados pessoais (LGPD) por agentes de tratamento no contexto eleitoral, Brasília: Tribunal Superior Eleitoral, 2021a. Available at: <https://www.tse.jus.br/hotsites/catalogo-publicacoes/pdf/guia-orientativo-aplicacao-da-lgpd.pdf>. Accessed May 18, 2022.

TRIBUNAL SUPERIOR ELEITORAL - TSE. **Aviso de Pauta: assinatura de acordo visa implementar a Identificação Civil Nacional (ICN)**. 15 mar. 2021b. Available at: <https://www.tse.jus.br/imprensa/noticias-tse/2021/Marco/aviso-de-pauta-assinatura-de-acordo-visa-implementar-a-identificacao-civil-nacional-icn>. Accessed May 12, 2022.

TRIBUNAL SUPERIOR ELEITORAL - TSE. TSE institui comissão para gerir o tratamento de inconsistências biométricas do Cadastro Eleitoral. [s.l.], 03 set. 2021c. Available at: <https://www.tse.jus.br/imprensa/noticias-tse/2021/Setembro/tse-institui-comissao-para-gerir-o-tratamento-de-inconsistencias-biometricas-do-cadastro-eleitoral>. Accessed May 18, 2022.

TRIBUNAL SUPERIOR ELEITORAL - TSE. TSE e CNJ realizam primeira ação para identificar pessoas sem documento nas prisões. [s.l.], 19 out. 2021d. Available at: <https://www.tse.jus.br/imprensa/noticias-tse/2021/Outubro/tse-e-cnj-realizam-primeira-acao-para-identificar-pessoas-sem-documento-nas-prisoes>. Accessed May 18, 2022.

TRIBUNAL SUPERIOR ELEITORAL - TSE. Contrato TSE nº85/2021. Contrato de prestação de serviços que entre si celebram o Tribunal Superior Eleitoral e o Serviço Federal de Processamento de Dados - SERPRO. 31 dezembro 2021e. Available at: <https://www.tse.jus.br/transparencia-e-prestacao-de-contas/licitacoes-e-contratos/contratacoes-diretas-2021/serpro/ct-85-2021-serpro/rybena_pdf?file=https://www.tse.jus.br/transparencia-e-prestacao-de-contas/licitacoes-e-contratos/contratacoes-diretas-2021/serpro/ct-85-2021-serpro/at_download/file>. Accessed May 18, 2022.

TRIBUNAL SUPERIOR ELEITORAL - TSE. TSE lança nesta terça (8) nova etapa de implementação do Documento Nacional de Identidade (DNI). [s.l], 07 fevereiro 2022a. Available at: <https://www.tse.jus.br/imprensa/noticias-tse/2022/Fevereiro/tse-lanca-nesta-terca-8-nova-etapa-de-implementacao-do-documento-nacional-de-identidade-dni>. Accessed May 18, 2022.

TRIBUNAL SUPERIOR ELEITORAL - TSE. Biometria atual por UF. [s.l.], 17 maio 2022b. Available at: <https://www.tse.jus.br/eleitor/biometria/biometria-atual-uf>. Accessed May 18, 2022.

UNIÃO EUROPEIA. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Available at: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679>. Accessed May 17, 2022.

UNIVERSIDADE DE BRASÍLIA. Relatório técnico: Características e Questões de Pesquisa sobre Gestão de Identidade, 2015. Available at: <https://www.justica.gov.br/Acesso/governanca/pdfs/infraestrutura-trecnologica/20150228-mj-ric-rt-caracteristicas-e-questoes-de-pesquisa-sobre-g-i.pdf/view>. Accessed May 17, 2022.

UNITED NATIONS. A/HRC/39/29: The right to privacy in the digital age - Report of the United Nations High Commissioner for Human Rights, 03 agosto 2018. Available at: <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/239/58/PDF/G1823958.pdf?OpenElement>. Accessed May 18, 2022.

UNITED NATIONS. A/74/48037: Report of the Special rapporteur on extreme poverty and human rights, 11 outubro 2019. Available at: <https://www.ohchr.org/Documents/Issues/Poverty/A_74_48037_AdvanceUneditedVersion.docx>. Accessed May 18, 2022.

VILAS BÔAS, Bruno. Sub-registro de nascimentos cede, mas ainda é desafio no Norte, diz IBGE. Valor, 04 dez. 2019. Available at: <https://valor.globo.com/brasil/noticia/2019/12/04/sub-registro-de-nascimentos-cede-mas-ainda-e-desafio-no-norte-diz-ibge.ghtml>. Accessed May 18, 2022.

WANGHAM, Michelle S, *et al*. Gerenciamento de Identidades Federadas. *In.*: Livro de Minicursos do X Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais, 2010, p.1-52. Available at: <https://doczz.com.br/doc/384142/mc1--gerenciamento-de-identidades-federadas>. Acesso em: 16 mai. 2022.

WIMMER, Miriam. Limites e Possibilidades para o Uso Secundário de Dados Pessoais no Poder Público: Lições da Pandemia. REVISTA BRASILEIRA DE POLÍTICAS PÚBLICAS (RBPP), v. 11, p. 123-143, 2021a. Available at: <https://www.publicacoes.uniceub.br/RBPP/article/view/7136>. Acesso em: 18 mai. 2022.

WIMMER, Miriam. Regime Jurídico do Tratamento de Dados Pessoais pelo Poder Público. *In*: MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JUNIOR, Otavio Luis (Org.). Tratado de Proteção de Dados Pessoais. 1ed. Rio de Janeiro: Forense, 2021b, p. 271-288.

ZANATTA, Rafael. A. F. Proteção de dados pessoais como regulação de risco: uma nova moldura teórica?. Anais do I Encontro da Rede De Pesquisa Em Governança Da Internet, 2017. Available at: <http://www.redegovernanca.net.br/public/conferences/1/anais/ZANATTA,%20Rafael_2017.pdf>. Acesso em: 10 mai. 2022.