RESEARCH REPORT

May 2024

Digital sovereignty: for what and for whom? Conceptual and political analysis of the concept based on the Brazilian context

FGV DIREITO SP
CENTRO DE ENSINO E PESQUISA EM INOVAÇÃO

Internet Society
Capítulo Brasil

CREDITS

CENTER FOR EDUCATION AND RESEARCH ON INNOVATION

CEPI FGV Direito SP

Coordination

Alexandre Pacheco da Silva

Marina Feferbaum

Head of Projects

Ana Paula Camelo

Researchers

Ana Carolina Rodrigues Dias Silveira

Ana Paula Camelo

Beatriz Yuriko Schimitt Katano

Laurianne-Marie Schippers

More information: http://bit.ly/cepidireitosp

INTERNET SOCIETY - BRAZILIAN CHAPTER

ISOC Brazil

President

Flávio Rech Wagner

Vice-Presidente

Raquel Fortes Gatto

Director of Projects

Pedro de Perdigão Lana

More information: https://isoc.org.br/

HOW TO CITE

CAMELO, Ana Paula et al. *Digital sovereignty:* for what and for whom? Conceptual and political analysis of the concept based on the Brazilian context. São Paulo: CEPI FGV DIREITO SP; ISOC Brasil, 2024.

LICENCE

Digital sovereignty [recurso eletrônico] : for what and for whom? : conceptual and political analysis of the concept based on the Brazilian context / Ana Paula Camelo ... [et al.]. - São Paulo : FGV Direito SP, 2024.
36 p.

Inclui bibliografia.
ISBN: 978-65-87355-59-7

1. Soberania - Brasil. 2. Tecnologia da informação - Aspectos políticos. 3. Inovações tecnológicas - Aspectos jurídicos. 4. Internet. 5. Proteção de dados. I. Camelo, Ana Paula. II. Silveira, Ana Carolina Rodrigues Dias. III. Katano, Beatriz Yuriko Schimitt. IV. Schippers, Laurianne-Marie. V. Silva, Alexandre Pacheco da. VI. Wagner, Flavio Rech. VII. Lana, Pedro de Perdigão. VIII. Gatto, Raquel Fortes. IX. Fundação Getulio Vargas.

CDU 004

Ficha catalográfica elaborada por: Cristiane de Oliveira CRB SP-008061/O
Biblioteca Karl A. Boedecker da Fundação Getulio Vargas - SP

TABLE OF CONTENTS

ABSTRACT

The concept of sovereignty has transformed over time. In a hyperconnected society, guaranteeing national sovereignty implies opportunities and challenges TO guarantee "digital sovereignty". However, different interpretations coexist around this concept, generating a polysemy that is little explored and has potential impacts. In the research “Digital sovereignty: for what and for whom? Conceptual and political analysis of the concept based on the Brazilian context”, developed by CEPI FGV Direito SP in partnership with ISOC Brazil, we seek to map and understand the different approaches to digital sovereignty in Brazil, considering its socio-technical, political and legal dimensions. The objective is to qualify the academic debate and decision-making on the topic, considering the rise of the most diverse initiatives based on the argument of Brazilian sovereignty and the resulting local and global impacts. The research is based on the hypothesis that these different narratives co-produce each other, impacting Internet governance.

I - INTRODUCTION

The idea of “sovereignty” is often mentioned as one of the characteristics of the formation of modern states and their ability to govern themselves without external interference or with less foreign interference. (Sousa, 2023). Over the years, the classic concept of sovereignty became connected, influencing and influenced by new elements that make up the reality of each era. This is the case with “digital”. In a situation where everything and everyone are, in a certain way, connected, the discussion around the idea of sovereignty emerges necessarily linked to initiatives and decisions related to digital infrastructures, technologies, data, the Internet and a range of other topics (Couture; Toupin, 2019). In the assessment of Professor of Intelligence Technologies and Digital Design at PUC São Paulo Dora Kaufman, “in a hyperconnected society, in which most communication and sociability occurs in digital environments or through digital devices, guaranteeing national sovereignty is, in part, ensuring 'digital sovereignty'” (Kaufman, 2023). However, even though several scholars on the subject present their understandings of the concept[1], this research is based on the hypothesis

[1] For example, in the definition of Stenio Santos Sousa (2023): “Digital Sovereignty refers to the ability of States to ensure control over the online environment (cyberspace), that is, to ensure that their rules are respected by the various participants in the online world. The expression concerns the control of data, standards and protocols, processes, services and infrastructure [...] [In] the context of digital technologies, the concept of digital or technological sovereignty has been the subject of debate, which can

that different meanings and narratives that define it coexist and co-produce each other, causing a little-known polysemy. Furthermore, an important debate is being established about how said understanding justifies or is justified by local needs and can generate impacts, sometimes unintended, in the spectrum of Internet governance.

In "Navigating digital sovereignty and its impact on the Internet" (2022), the Internet Society already sought to systematize how different visions of sovereignty in cyberspace were projected through different political, regulatory and technological instruments. By analyzing government policies from different countries (such as Australia, China, India, Vietnam, South Africa, Rwanda, Nigeria, Russia and the European Union) that were explicitly linked to digital sovereignty, the document shows how "digital sovereignty policies can adversely affect how the Internet works and, more importantly, our ability to use the Internet" (Internet Society, 2022).

CONCEPT OF SOVEREIGNTY IN DISPUTE AND CONTINUOUS CONSTRUCTION

The notion of "digital sovereignty" is historically associated with attempts by undemocratic governments to patrol Internet operations and resources within their borders. In international policy discussions, the concept has been used to challenge existing approaches to Internet governance that rely on decentralized and multilateral processes. Currently, "digital sovereignty" is being used more widely in varied contexts around the world and for different purposes. That can include political interventions to give people and groups more control over information, but also measures that give justice and interior ministries direct control over daily internet traffic (Internet Society, 2022).

Taking the complexity of the issue as an assumption (Stirling, 2010), this report[2] aims to map and understand the different approaches and nuances in dispute over digital sovereignty in the Brazilian context. Deepening its socio-technical, political and legal

be understood as the national capacity to control over its own data and digital infrastructures, with little or total independence from large corporations or foreign governments".

[2] This report is one of the outcomes of the research "Digital sovereignty: for what and for whom? Conceptual and political analysis of the concept based on the Brazilian context", the result of the partnership CEPI FGV Direito SP and ISOC Brazil, with funding from ISOC Foundation.

dimensions, it seeks to qualify the academic debate and decision-making on the topic, considering potential impacts at both the local and global levels and taking into account the rise of debates and proposals whose justification is linked to Brazilian sovereignty.

II - METHODOLOGICAL STRATEGY

The data and information qualitatively analyzed in this document were collected from different sources, namely: (i) mapping and reading of national and international texts and documents; (ii) interviews with actors from different sectors of the Brazilian digital ecosystem; (iii) participation in events on the topic; (iv) free course classes on digital sovereignty[3], among others.

Although the bibliographic and documentary research effort was based on different strategies, sources, materials and search tools, it is important to recognize that this study may face limitations as it does not propose to present an exhaustive mapping of the subject. The fact that many documents do not explicitly present the term “digital sovereignty”, but deal with related themes and issues, may be one of the causes of possible limitations. Furthermore, at first it was decided not to use the combination of words “technological sovereignty”. The aim was to identify to what extent the discussion about “digital sovereignty” took place on its own.

Mapping of written documents on digital sovereignty

Throughout the project, a total of 180 documents were mapped that, directly or indirectly, dealt with the intersection between the digital ecosystem and national (digital) sovereignty. The documents consist of laws, bills, news, papers, scientific articles, among others. This set of publications was read and coded using a codebook built specifically for the research in order to identify subthemes and recurring debates around the concept of digital sovereignty.

[3] The course was offered between November and December 2023 free of charge. The objective was to qualify the debate and deepen the participants' skills to participate in debates and disseminate information related to the topic of digital sovereignty based on the Brazilian context and in dialogue with the international agenda. For further information, refer to the APPENDIX.

Some keywords and combinations were used for this mapping in the Google search field and within the specific domains of government bodies, research centers dedicated to Internet governance themes, websites of civil society organizations, technical bodies and multi-stakeholder forums, namely: “soberania digital”; “sovereignty + Internet + brazil”; “sovereignty + cyberspace + brazil”; “digital sovereignty + brazil”; “fragmentação da Internet”; “fragmentação da rede”; “Internet fragmentation + brazil”; “soberania + dados”; “soberania + Internet”; “soberania + ciberespaço”. There was no time filtering or filtering by type of document. Therefore, articles, *papers,* news, laws, bills, open letters, book chapters, reports, among others, were selected. Texts were selected only in Portuguese and English, in line with the choice of keywords. The following were disregarded in the analysis: texts (i) that dealt with digital sovereignty in a very generic way, without delving into the Brazilian scenario; (ii) that dealt with digital sovereignty in countries other than Brazil, (iii) that had at their core issues not related to digital sovereignty; (iv) written in languages other than English or Portuguese; (v) that mentioned sovereignty at one point, but did not have it as a relevant subject.

After applying the criteria indicated above, the resulting sample was coded by two researchers using the Atlas.TI software. In a second moment, a validation phase was carried out between the coding carried out in the previous stage, in order to correct any discrepancies in the application of the codes.

Semi-structured interviews

Semi-structured interviews were carried out with *stakeholders* working in different sectors of the digital area in Brazil in order to map and deepen perceptions and narratives that underpin their conceptions of digital sovereignty and its impacts.

The interviews constituted an important stage of interaction with actors in the Brazilian digital ecosystem to deepen understanding of the debate. At the beginning of the project, the goal of 15 interviews with people who work and/or research the topic of digital sovereignty was established, taking into account the following diversity criteria: (i) gender; (ii) region of Brazil in which the person resides/works; (iii) race; (iv) sector of activity (academic community, government, business, civil society, technical community).

The “Snowball” method was used throughout this process. At the end of each interview, the researchers asked the interviewee if he or she had recommendations considering the desired profile, which resulted, in turn, in the inclusion of new names in order to guarantee the desired diversity.

The question guide prepared was approved by the Research Ethics Committee of Getulio Vargas Foundation. It contained questions related to understanding the concept of digital sovereignty, current movements of different powers on the topic and the interaction of such public agents with the private sector. Questions were also asked about the international scenario involving digital sovereignty.

Data coding and analysis

The first version of the "codebook" used to code the documents mapped and semi-structured interviews was written based on the analysis of the texts that served as inspiration for the preparation of the project. Said texts are part of a preliminary bibliography presented with the project. The codes were used to streamline qualitative analysis regarding the topic.

A test phase of the codes that make up the book was carried out. The code definitions underwent changes when they needed to better adapt to the contexts found in the literature. The advanced version of the codebook was completed after two testing phases. It is noteworthy that, as reading and coding progressed, new codes were included after assessing their relevance.

From the application of the codes, it was possible to understand which themes about digital sovereignty appear most frequently, which sectors certain interpretations were associated with, what are the points of attention that should be taken into consideration when talking about the topic, what are the current challenges in Brazil, among others.

III - BRAZILIAN AGENDA OVERVIEW

Incidence of the theme in the Brazilian scenario

In Brazil, the topic has been gaining greater prominence in different spaces and involving all sectors. The growing incidence of the topic in multistakeholder forums on Internet governance, such as the Brazilian Internet Forum (FIB), exemplifies this projection. FIB has been counting on workshop submissions on digital sovereignty since its 11th edition (2021). In 2023, the forum featured 2 workshops on the subject, a main session and the ISOC Brazil annual meeting, which took place within the event's agenda and also addressed the topic. Furthermore, other informal spaces for discussion can be mentioned, expanding opinions from different sectors and perspectives

that reflect the opportunities and challenges of digital sovereignty in Brazil. For the 14th edition, to be held in the city of Curitiba in May 2024, 14 workshops were proposed covering the theme, among which 3 were selected. In addition, the event will feature a parallel activity organized by the Internet Governance Research Network with the title “Disorganizing I can organize myself: digital sovereignty and technodiversity on the peripheries of capitalism”. The topic will also be part of the ISOC Annual Meeting, on Day 0 of the event.

Still at the local level, a public consultation mobilized by the Internet Steering Committee (CGI) regarding the regulation of digital platforms in 2023 stands out. The objective of the consultation was to map different types of digital platforms, identify risks associated with the use of platforms and point out regulatory measures capable of mitigating such risks and identify possible actors and paths for regulation (CGI Public Consultation, 2023, p. 22). The initiative included 1,320 contributions from 140 participants (individuals and organizations) from the government, third sector, business and scientific and technological communities, and raised relevant reflections on digital sovereignty. Different conceptions of the concept were highlighted, namely (i) State control in relation to the layers of the digital environment and in relation to national security and data flow; (ii) development of local technologies to reduce dependence on foreign companies; and (iii) autonomy and self-determination of individuals, allowing people to make their own decisions about what is done with their information (CGI Public Consultation, 2023, p. 16). The three approaches mentioned are in line with the results of this research, and will be presented in this document, regarding the polysemy of “digital sovereignty”.

At the legislative level, some bills stand out in the debate on the topic. Bill (PL) 2630/2020, which proposes the regulation of digital platforms in the country and establishes rules for content moderation and intermediary liability, is one of them. PL 2768/2022, which also proposes the regulation of platforms, focuses on economic regulation, and PL 2338/2023 deals with the use of Artificial Intelligence in Brazil. They all present important dimensions regarding the regulatory perspective and the search for a balance of national/local interests and demands in the face of global movements and structures (which should, in theory, adapt to the Brazilian reality). That would guarantee users' rights and streamline the exercise of jurisdictional power, in the view of many experts. Still in the legislative debate, it is worth mentioning the holding of public hearings and debates with experts to address the “role and limits of the country in the construction of legislation that concerns a global mechanism that is the Internet” (Brazil, 2022), exploring in a dedicated manner PL 2630/2020 through the lens of digital sovereignty.

The issue is also present in the Judiciary. Many matters related to the functioning of the Internet and digital tools, such as platform accountability, international data transfer, among others, have been discussed, as they end up impacting Brazilian jurisdictional power. At the Federal Supreme Court, the Declaratory Constitutionality Action n.º 51 stands out, declaring the constitutionality of the Mutual Legal Assistance Treaty (MLAT) for requesting information directly from foreign platforms and Internet providers with headquarters or representation in Brazil (already final). The extraordinary appeals that discuss the constitutionality of art 19[4] of the Brazil's Internet Bill of Rights (MCI – Law n.º 12.965/2014) are worth highlighting, as well as the need for intervention by the Judiciary as a requirement to hold application providers responsible for content generated by users (still under trial)5.

The Superior Electoral Court, in turn, has participated in this debate through initiatives that seek to protect the electoral process from threats posed by the inappropriate use of social networks and the Internet, a central issue in the topic of regulating digital platforms in Brazil. While the Supreme Court discusses the constitutionality of the current regime for accountability of intermediaries and the Congress fails to reach a consensus on regulatory guidelines, the Electoral Court already holds providers responsible for disinformation content during electoral periods through Resolution n.º 23.610/2019. In March 2024, the Court promoted changes to the Resolution, including the regulation of content produced through Artificial Intelligence.

No less important, it is worth mentioning the coordination of third sector groups and people from different backgrounds on the subject. The Digital Sovereignty Letter,[6] addressed to Luiz Inácio Lula da Silva, then candidate for President of the Republic in 2022, is the result of this movement and was signed by researchers, professors and activists from across the country. At the heart of this document, which was presented in "defense of an emergency program for digital sovereignty" (Lavits, 2022), was the criticism of the market concentration model represented by *big techs* and the demand

[4] The art. 19 of the MCI determines that "the Internet application provider may only be held civilly liable for damages resulting from content generated by third parties if, after a specific court order, it does not take measures to, within the scope and technical limits of its service and within the deadline, make the content identified as infringing unavailable, except for legal provisions to the contrary," aiming to ensure freedom of expression and prevent censorship in accordance with the norm.

[5] Recently, there began to be a broader questioning, pointing to an alleged obsolescence of the MCI, which demands attention.

[6] More information at: https://cartasoberaniadigital.lablivre.wiki.br/carta/.

for the development of a national technological infrastructure to overcome the country's structural inequalities.

In addition to the increasing relevance of the topic in the Brazilian scenario, it is interesting to highlight Brazil's participation in international forums, such as the *Internet Governance Forum* (IGF). In the 18th edition of the IGF, held in Kyoto, in 2023, 4 workshops were held on the topic, of which 3 had the participation of representatives from Brazil.

It is believed that this movement will expand even further considering the number and diversity of existing initiatives linked to the topic[7], demanding continued monitoring and the participation of different voices in this debate. This impacts everyone at the local level and may have repercussions in other countries, given Brazil's enormous relevance when it comes to regulating the digital environment (such as the Civil Rights Framework for the Internet and the General Data Protection Law).

IV - Meanings of sovereignty in (de)construction

Different conceptions of digital sovereignty in the Brazilian debate

The multiplicity of understandings surrounding the concept when it comes to digital technologies and the Internet has already been mapped and explored (Internet Society, 2022). However, without analyzing the Brazilian situation, which is the purpose of this research.

The coding and analysis of the texts mapped and the interviews carried out supported the hypothesis that there is still no single meaning or understanding for the term “digital sovereignty” in the Brazilian debate. A variety of interpretations and narratives were identified that coexist linked to the term and its practical consequences. The difficulty to define the concept, by many sources, illustrates this complexity and diffusion of

[7] Among countless initiatives that are multiplying addressing the topic, the digital dossier entitled “Technological sovereignty and digital sovereignty”, organized by the Institute for Digital Development for Latin America and the Caribbean (IDD LAC), available at: https://iddlac.org/pt/soberania-tecnologica-e-soberania-digital/; the collective *Rede pela Soberania Digital / Network for Digital Soberania*, created in 2023 and which brings together militant entities and people around the topic, available a: https://soberania.digital/; and the research carried out by the *Data Privacy Brazil Research Association* on the topic of Internet fragmentation and digital sovereignty, with support from *Global Partners Digital*, cf. https://www.dataprivacybr.org/projeto/fragmentacao-da-internet-e-soberania-digital/.

perspectives, especially because the term can take on different meanings depending on the area in which it is interpreted.

The survey respondents were also unanimous in the opinion that "digital sovereignty" is a concept in dispute, and that its meaning may vary depending on the context, even if it is from a national perspective. The following excerpt was taken from a conversation with an interviewee from the academic community, and expresses the importance of the discussion today, even though it is not possible to reach a single definition:

> I would say the concept at this moment, for me, at least as a researcher, matters less. **What matters more is the meaning it has in Brazil's positioning in the face of geopolitics that today is marked by disputes around the development of science, technology in the field, mainly digital**. For me, digital sovereignty concerns a nation, a country, that intends to take over international leadership as a producer of science, technology and digital solutions. Such solutions, aimed mainly at the economic **development of said country, at the reduction of inequalities and the creation of a bloc of countries, in this case of the Global South**. This bloc can face the technological advancement that occurs mainly within large private companies, even more than in nations, in States, even more than, say, at the state level of these countries. And mainly the development of technology, which takes place in the private field, so that we can have some technological self-determination based on the economic, political, social and cultural arrangements specific to our region/country. (Emphasis added.) (Interview SD135.)

Being digitally sovereign can mean less dependence on technologies from foreign companies, based mainly in the Global North, the ability to make decisions about the control of critical infrastructures and national security, greater knowledge about the management of their data by citizens, among others.

Sovereignty, in the first instance, appears to be a strategic state instrument to defend the country's interests and to enforce its laws when in conflict with those of other countries, or in the face of threats to local needs, particularities and values. However, sovereignty as autonomy cannot be left in the background, from the point of view of the individual or groups of individuals, as an instrument of access to fundamental rights (e.g., self-determination, data protection, privacy, among others).

It is important to highlight that this work does not propose to exhaust meanings in (de)construction that can be attributed to digital sovereignty in the national debate. The research aims to identify and systematize some of these possibilities that can

contribute to better understanding the topic itself and its impacts. It is of great importance to recognize that different interpretations do not necessarily contradict each other, but often complement each other.

TABLE 1 – DIGITAL SOVEREIGNTY PERSPECTIVES/OBJECTIVES MAPPED IN THE BRAZILIAN CONTEXT

National security and ability to enforce laws	**Economic self-determination**
• Fight against threats to national security (foreign cyberattacks and online vulnerabilities). • Guarantee of digital dominance within borders through the ability to establish and enforce laws within its territory (from critical infrastructure to the use of Internet technologies in political processes and changes). • Lawful access to information by law enforcement agencies, competition authorities and other regulators; local data control. • Influence on the functioning and operation of services and software in its territory.	• Strengthening of the development of local industry to compete in environments dominated by foreign technology companies. • Strong protectionist measures that foster market forces aiming for a more balanced environment.
Protection of rights and qualification of citizens/users and communities	**Defense of social norms and values**
• Strengthening of individual and collective autonomy in relation to technological platforms. • Empowerment of citizens and communities to take action and make decisions related to their data and digital activities.	• Preservation and/or encouragement of certain local norms and traditions to promote social, cultural and political values from third parties. • Data localization policy to assert citizens' rights over their data and security and privacy measures against data stored abroad. • Data localization policy to support the actions of intelligence actors and law enforcement agencies.

Source: based on INTERNET SOCIETY. *Navigating digital sovereignty and its impact on the Internet*. December 2022. Available at: https://www.internetsociety.org/wp-content/uploads/2022/11/Digital-Sovereignty.pdf. Accessed in May 2024.

An interesting proposal to organize possible meanings of digital sovereignty that deserve to be highlighted was presented by an interviewee from the third sector. According to her, digital sovereignty can manifest itself in three fields: (i) technical; (ii) legal and (iii) political. The technical field involves more complex questions about the physical functioning of digital infrastructure. This dimension implies the existence of structures that give materiality to the operation of technologies, making digital sovereignty feasible. The legal and political dimensions are strongly linked, and are fundamental to understand the reality of the Global South, which is still highly dependent on developed countries because of its colonial past. The legal aspect emerges associated with laws and other regulatory mechanisms that affect the Brazilian scenario. However, regarding this last dimension, it is not enough for such instruments to exist; there needs to be *enforcement*, which, as pointed out by the interviewee, is not sufficiently present in Brazil. Even though the country has laws that are a reference throughout the world, their compliance is not guaranteed due to several factors. This means it is hard for Brazil to position itself as digitally sovereign in some aspects. Finally, the political dimension is related to the decisions taken by representatives of the Brazilian State and which define Brazil's position in relation to other countries. Therefore, it is about the impacts of governments' political choices, and how rapprochement with other nations and their companies is carried out. (Interview SD140.)

Legal and political aspects are strongly connected, since the existence of national regulatory instruments needs to be in line with supervision to guarantee compliance by foreign countries. If *players* wish to operate in the Brazilian market, it is important they follow local legislation, so that Brazil can assert its interests and get closer to sovereignty also from a digital point of view.

Below, some of the nuances related to these three main dimensions mentioned by the interviewee will be explored..

Digital sovereignty and infrastructure

Infrastructure is essential for the operation of technologies and applications, both those developed in Brazilian territory and those from other countries. Therefore, for a country to be digitally sovereign, it is not enough to be able to produce free software if the necessary independence is not available in terms of infrastructure for the software to be operated and to function properly, for example. The lack of investment and the impossibility of using more complex local infrastructures, such as *data centers*, is one

of the aspects that raise concerns about the transfer and processing[8] of strategic and sensitive data from different areas considered to be of national interest and which would not be under the control of the country itself. In the assessment of a representative of the academic community:

> I'm talking about software, data, source code here, but one thing we really need to think about is the structure. Because even if we have open source, our own data, [...], we have a very precarious infrastructure to connect and install servers in the country; that would make us install our systems abroad. [...] So, we leave their service platform, but enter their infrastructure platform. So, I actually argue that, especially for the nation's critical data, this should be managed, supported by the nation, by the country, by its companies. [...] We need to discuss the issue of sovereignty reinforced with infrastructure, both in terms of connections and the availability of high-speed servers, of servers [...] with high storage capacity. (Interview SD153.)

Likewise, another actor from the same sector highlighted the importance of infrastructure for digital sovereignty:

> The State will need to invest in infrastructure. I can't set up *data centers* without public investment. Therefore, strengthen companies and federal entities, like Dataprev, like Serpro, so that they are places where you can invest in *datacenters* and storage. In parallel there is the issue of education. Universities indeed need to invest more in research and development of technologies. I would say that will take a little longer; we will have to wait a few generations before we can actually produce and promote new technologies. (Interview SD156.)

Informational sovereignty and self-determination

From the discussion of information management by the State and by citizens and national institutions, it is possible to identify the perspective of informational sovereignty, which presents a double complementary interpretation. A digitally sovereign country is considered to be capable of controlling the use of such information without depending on other countries and without being subject to foreign interests. This narrative is also associated with encouraging access to digital knowledge by citizens. That makes

8 Art. 5 of the LGPD (General Data Protection Law): “For the purposes of this Law, processing is considered [...] X: any operation carried out with personal data, such as those relating to collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, archiving, storage, elimination, evaluation or control of information, modification, communication, transfer, diffusion or extraction;”.

them better able to understand the relevance of the topic and to individually consider the management of their own information, the necessary care and associated risks.

Below is an excerpt taken from the speech of an interviewee from the government sector about the importance of information for the concept of digital sovereignty:

> Because the topic that structures us, if we were to think of a more tangible term, would be... I would call it "information integrity". And the integrity of information is directly linked to our ability to guarantee sovereignty, because if there is no sovereignty, we cannot have informational integrity within our country, because that would be compromised by the interests of other countries. (Interview SD157.)

Regarding the spectrum of informational sovereignty related to the individual, an actor from the academic community highlighted the following:

> When we talk about digital sovereignty, I would link it to the idea that the country has the conditions, and the people in particular have the conditions, to collectively manage their reality in the information society, don't they? They would also manage their digital culture, in a sovereign way. So, that is, making legal and political, technical and economic decisions in relation to your own reality, right? With autonomy, with freedom. Without being subject to the interests and limitations of other countries. (Interview SD113.)

Cybersecurity and national security

Digital sovereignty is also recurrently associated with national security issues. A digitally sovereign country would be able to protect itself from external attacks and excessive interference by third parties, especially by major world powers. To Lucca Belli *et al*. (2023), the discussion on digital sovereignty takes place together with the most diverse initiatives that propose the promotion and definition of the desired digital transformation model.

> Indeed, the adoption of digital technologies can enable huge advances to be put at the service of people, but it can also be set against individuals, companies and nation-states. From this perspective, it seems natural to consider the enormous and constantly growing overlap between digital sovereignty and cybersecurity. (Belli *et al*., 2023, p.46).

The following excerpt was taken from the interview with a *stakeholder* from the government sector, and highlights the relationship between digital sovereignty and the defense of Brazil's national interests, preventing submission to foreign powers:

> The idea of cyber warfare, for example. And obviously, when we think about defense strategies against these types of attacks, about creating national policies, national cyber defense strategies, the issue of digital sovereignty always underlies there. It is very hard to think of a truly robust cyber defense policy with a heavy dependence on foreign technologies. The more dominance... let's say, the more we manage to develop these technologies nationally, the greater our... let's say, the better our cyber defense capacity will be. (Interview SD154.)

In addition to the main perspectives presented so far, it is possible to identify some developments in the debate that go beyond and connect the dimensions presented above. Such nuances will be named below, without presenting an independent interpretation of the concept.

Cross-cutting debates

Independence from foreign companies

The need to build Brazilian independence in relation to foreign companies is mainly linked to the fact that the country uses many digital services provided by multinational companies based in developed countries. This reflects numerous challenges regarding the sovereign development of national technologies and infrastructure. This phenomenon can be noted in schools, universities and research centers, for example, as well as in healthcare institutions, which, despite storing extremely valuable sensitive data, depend on foreign infrastructure to operate.

Development of technologies, impacts on the economy and competition

Another frequently mentioned aspect is the intrinsic connection between sovereignty and the development of technologies to empower the Brazilian market. Encouraging the production of national technology is, in the assessment of different actors, essential for the country to achieve digital sovereignty, as in this way, it will be able to operate in the digital market, which is still extremely restricted to a few already consolidated *players*.

Through incentives for the development of local technology, it is possible that Brazilian companies will be able to start exploring the market, causing dependence to decrease. This could also impact on the reduction of costs for certain technologies, which would benefit both the State, which could start using national technology to store its data and

process it, for example, and citizens, who would have access to Brazilian technology at a lower cost.

Jurisdiction and regulatory power

The relationship between sovereignty, issues of jurisdiction and regulatory power occurs because digital sovereignty is one of the instruments capable of reinforcing the autonomy of the Brazilian State in relations with other countries. As the digital medium is not restricted to geographic borders and is globally connected means that, in several situations, two or more jurisdictions are in conflict, with policies and laws dictating different rules for a given case. The power to regulate is often used to ensure that Brazilian laws are applied and prevail, especially in relation to foreign companies that operate and/or wish to enter the Brazilian market. However, it is worth highlighting that excessive sovereignty measures can affect the global functioning of digital tools, as they are capable of generating fragmentation of the Internet or user experience, or even limiting access to the Brazilian market.

Digital sovereignty from the perspective of individual empowerment

The association of digital sovereignty with the possibility of exercising human and fundamental rights, such as the right to self-determination of people, privacy and consumer rights, presents itself as an important complementary dimension. Digital sovereignty is used, in these cases, as a tool that allows the empowerment of society, through greater access to information. This enables to expand the perception of their own rights, allowing people to know more about their reality and become capable of fighting for their rights.

For this reason, in order to achieve digital sovereignty, investment in education for digital reality would be essential. This makes people more aware of the challenges and opportunities of the digitally connected market. It is important to invest in training citizens to use digital tools that, nowadays, can be valuable instruments to expand democracy.

This means that having advanced technologies and infrastructure in the country is not enough; It is also necessary to educate the population so that they are able to take advantage of these elements. It is necessary to invest in the expansion of digital knowledge, as it allows individual rights to be demanded more efficiently. An example

is the use of technologies to disseminate information and take over spaces for debate by historically marginalized populations. In the assessment of a representative of the academic sector:

> ...from the strictest point of view of the concept, I also advocate more for the idea of popular digital sovereignty. Therefore, emphasize precisely the democratic character and legitimacy, which involves the population's participation in self-determining the direction of scientific and technological development. Then, it doesn't matter if it's from a city, a state, a country in the global south or the world as a whole, but, above all, giving visibility to those who historically have no voice. So, I think it is a concept necessarily linked to the democratic aspect, that follows a larger geopolitical trend. (Interview SD152.)

This perspective is intrinsically related to other dimensions of the debate already presented, such as: the need to develop our own and, preferably, open infrastructures, which guarantee greater control over the storage and processing of users; informational sovereignty, through the reduction of informational asymmetries; and the notion of users' self-determination regarding the use of their data. In the words of a representative of the academic sector,

> Look, digital sovereignty is related to how our data and the technology that is developed is managed by an entity, by a body, by a government, by a nation, without depending on other governments and other nations. And really “depend”, in the sense of [...] technological dependence. For example, if we have our own data, if we use systems that are provided by institutions not related to the state, or that are actually related to other nations, to other states, then this shows that we have little digital sovereignty, and that we are technologically dependent. (Interview SD153)

Balance of the debate

It is not possible to guarantee, in advance, that all these concepts and dimensions of the debate can go together in practice, especially when “state” and “individual” perspectives are compared. It is therefore necessary to seek balance between expectations and impacts of initiatives linked to the idea of digital sovereignty. If, on the one hand, the lack of measures towards national protection can be considered worrying for a country due to possible and unwanted vulnerabilities, on the other hand, the excess of measures justified through this concept can generate negative repercussions for the economy, national security itself, citizens' rights and relations between people, institutions and countries. It is important to be clear about the *trade-offs* of actions guided by each perspective.

An example of the undesirable impacts that are much discussed and that emerge from excessive local protective measures is their potential for repercussions on the functioning of the Internet, which in turn is based on the principles of open, globally connected, safe and reliable Internet for all people. One country's laws may contain too much specificity related to local realities, which makes compliance by other countries more challenging. This obstacle to the adaptation of foreign nations can be considered harmful by fragmenting the Internet at the technical level and/or user experience.

ABOUT INTERNET FRAGMENTATION

The *White Paper* "*Internet fragmentation: an overview*" (Cerf *et al.,* 2016), from the World Economic Forum, lists three forms of fragmentation:

Technical fragmentation: conditions in the underlying infrastructure that prevents systems from fully interoperating and exchanging data packets, and for the Internet to function consistently across all endpoints.

Government fragmentation: government policies and actions that limit or prevent certain uses of the Internet to create, distribute, or access information resources.

Commercial fragmentation: commercial practices that limit or prevent certain uses of the Internet to create, distribute or access information resources.

The *IGF 2022 Policy Network Internet Fragmentation* (2022, p. 14-15), in turn, classifies the phenomenon of fragmentation into:

User experience fragmentation: which results in a different Internet user experience depending on where users are accessing (or not accessing) it.

Fragmentation of the technical layer of the internet: related to the interoperability of the Internet, and which can be caused by interference by the creation of "national Internets" limited within geographic borders; or by routing traffic through private infrastructure linked to large technology companies.

Fragmentation of Internet governance and coordination: tied to a lack of global commitment and structure across multilateral and multistakeholder forums, governments and stakeholders to address global Internet policy issues from a human rights and free-flow data perspective.

This problem occurs when there is a big difference between the jurisdiction of the place where the company wants to operate and that of its country of origin. In short, due to this discrepancy, certain activities carried out by the company are permitted in one location but not in another, meaning that content shared on the Internet is not homogeneous. As a result, some users in certain regions have no access to some content, while it is made available to other users, which can trigger, in turn, a series of unwanted events that weaken duties and rights.

An example that demonstrates how much Internet fragmentation can occur as a result of sovereignty initiatives is the case of the Internet Sovereignty Law in Russia. This law delegates authority to a public agency, which allows filtering traffic on the country's networks by intermediary servers. The measure goes against the critical property of decentralized management of routings between networks. Simply put, this situation is worrying because a person connected to an Autonomous System, in theory, should be able to connect to all the networks they want. However, this is not what happens because there are intermediaries that control traffic, preventing certain content from reaching users in the country and negatively impacting on the Internet structure (WAGNER, 2023).

V - LEGISLATIVE DEBATE

Recognizing the importance of legal instruments to impose conditions and requirements in favor of digital sovereignty in the form of regulation, this research mapped and analyzed 36 federal bills (PLs) aiming at identifying proposals that connect with the debate. It was observed that the majority of legislative projects do not expressly mention the topic, but reflect aspects related to it, such as the need for its own technological development; local regulation and exercise of jurisdictional power; protection of users' rights; protection of institutions and the democratic process, among others.

Among the oldest mapped Bills, it is noted there was a tone of optimism regarding the use of the Internet. In recent years, however, Brazilian legislators have also begun to

consider the risks and threats offered by the network. If until the mid-2010s digital technologies were seen as instruments to promote digital citizenship, from the second half of that decade onwards there seems to be a breakdown in trust; projects start paying attention to risks, including those to democracy. On the other hand, it is noted that the legislator remains concerned with guaranteeing freedom of expression. This concern is manifested in several Bills.

Table 1 presents the list of Bills analyzed (from oldest to most recent).

Table 1 – List of legislative projects analyzed

Bill (PL)	***Legislative House***
PL 4219/2008	*Chamber*
PL 4805/2009	*Chamber*
PL 2024/2011	*Chamber*
PL 6114/2013	*Chamber*
PL 6827/2013	*Chamber*
PL 7682/2014	*Chamber*
PL 730/2015	*Senate*
PL 267/2016	*Senate*
PL 6413/2016	*Chamber*
PL 7574/2017	*Chamber*
PL 9115/2017	*Chamber*
PL 11119/2018	*Chamber*
PL 67/2019	*Chamber*
PL 2262/2019	*Chamber*
PL 3582/2019	*Chamber*
PL 4027/2019	*Senate*
PL 4381/2019	*Chamber*
*PLP 243/2019**	*Senate*
PL 6455/2019	*Chamber*

PL 487/2020	*Senate*
PL 2630/2020	*Senate*
PL 2891/2020	*Senate*
PL 4510/2020	*Chamber*
PL 4939/2020	*Chamber*
PL 5179/2020	*Senate*
PL 199/2021	*Chamber*
PL 2270/2021	*Chamber*
PL 112/2021	*Senate*
PL 199/2021	*Chamber*
PL 397/2022	*Chamber*
PL 714/2022	*Chamber*
PL 1515/2022	*Chamber*
PL 2529/2022	*Senate*
PL 2768/2022	*Senate*
PL 2790/2022	*Senate*
PL 2338/2023	*Senate*

*Complementary bill.
Source: prepared by the authors.

The proposals turned out to be quite diverse, addressing different themes covered by the debate on digital sovereignty. There was also an increase in the number of projects from 2019 onwards, which proves the need for continuous monitoring. The main themes and focuses covered by the Bills mapped are described below.

Economy and competitive market

It appears that, in recent years, proposals have been presented addressing competition aspects that were not previously on the Brazilian legislator's radar, especially related to the actions of content providers. Among these proposals, PL 397/2022 and PL 2768/2022 stand out, both influenced by the debate surrounding the Digital Markets Act (DMA) in Europe. In addition to competition issues, the legislator is concerned

about the level of competitiveness of the internal technology market in the face of the global market. PL 6413/2016, for example, expresses this concern.

Technological development and economic independence

Still within the scope of economic concerns, projects such as PL 6413/2016 were identified, which proposes investments in infrastructure to promote national technological development and the installation of *datacenters* in Brazil. The project states that these measures could prevent problems related to traffic control and data storage of Brazilian users – concentrated on foreign servers – and would generate qualified jobs.

Power of jurisdiction

Bills were identified addressing the need to regulate intermediary providers and concerns about issues related to conflicts of jurisdiction. In PL 397/2022, for example, the legislator draws attention to the risk of harming the protection of legal assets of Brazilian citizens and companies, highlighting the importance of providers having formal representation in the country, in order to respond civilly and criminally for acts carried out under Brazilian jurisdiction.

PL 730/2015 is another example of a bill addressing the issue. It warns of the difficulty of ensuring compliance with court decisions against foreign intermediaries, especially due to the location of the servers where user data is stored. This and other legislative projects highlight the difficulty of punishing crimes committed over the Internet.

Citizenship

It was found that, in the period from 2008 to 2019, there were several projects proposing the adoption of digital technologies to modernize democratic mechanisms and, thus, facilitate the exercise of citizenship and increase popular participation in government decisions. However, as of 2020, bills with a different focus were identified. Digital media, especially social networks, are now seen as threats to the health of the democratic process. In this sense, propositions emerge making providers and users responsible. That is the case, for instance, of PL 2630/2020 and PL 714/2022.

Exercise and protection of rights

Many legislative projects propose the adoption of mechanisms that promote popular participation in decision-making and electoral processes through digital instruments. In other words, they seek to promote "popular sovereignty" through "digital citizenship". This is the case, for example, with PL 7574/2017, PL 67/2019 and PL 4805/2009. PL 714/2022, however, is an example of a bill that provides clear provisions to protect the rights of users of services offered over the Internet, establishing responsibilities for providers.

Cybersecurity

Security and trust in electronic systems are central to many legislative proposals. There is a concern with preventing and combating crimes, but also with national defense. PL 1515/2022 is an example of a proposal that addresses these issues.

In one of the legislative projects (namely, PL 6413/2016), mention is made of Edward Snowden's revelations, from which it became known that the Brazilian State was a victim of espionage. Developing our own information technology and controlling over the flow of data are seen as strategic.

Featured bills

Among the 36 legislative projects mapped and analyzed, 3 stand out and are detailed below.

PL 2630/2020[9]

Currently, the regulation of digital platforms is one of the most relevant topics in discussions about the exercise of digital sovereignty, given the reach and economic power acquired by *big techs*, as opposed to state power. Furthermore, several actors interviewed in the research highlighted the regulation of platforms as one of the central themes in the country's current digital governance agenda. This regulatory pressure

[9] PL 2630/2020 was approved by the Federal Senate in June 2020. It is currently being processed in the House of Representatives, where the text has undergone significant changes and important advances in technical and legal terms. However, there are still controversial aspects that deserve attention. In April 2024, the House President announced the creation of a working group to discuss the matter, generating uncertainty about the future of the agenda.

is a reflection of the crisis of trust in networks, driven by the spread of hate speech and disinformation content, which pose as threats to rights and create risks to the democratic order.

The proposal to regulate this matter with the most advanced processing in the Brazilian National Congress is PL 2630/2020 (also known as “Fake News Bill”). The project establishes content moderation rules on social networks and messaging services and changes the platforms' liability regime. It has parallels with the European Union's Digital Services Act (DSA), which came into force in December 2020, providing for intermediary service providers to implement a series of measures to protect their users against online threats related to disinformation, hate speech , terrorism and child exploitation. Like the Brazilian legislative project, DSA creates transparency rules (including on content moderation policy and the functioning of algorithms), and establishes guarantees for users, such as the right to appeal against moderation decisions and to be informed about how your data is used and protected.

PL 2630/2020 FROM THE PERSPECTIVE OF SOVEREIGNTY: the analysis of PL 2630/2020 allows us to identify different dimensions of digital sovereignty, among which the following stand out: (i) the ability of the State to enforce its own laws, which is directly related to the regulatory power and the exercise of national jurisdiction; and (ii) the promotion and protection of users' rights (through rules that promote informational sovereignty and self-determination of personal data, for example), which reflect the individual perspective of this debate.

PL 2768/2022

PL 2768/2022 appears as an alternative proposal to PL 2630/2020, abandoning the issue of content moderation and proposing economic measures for the regulation of digital platforms.

It is also inspired by the European debate, but is closer to the Digital Market Act (DMA), which came into force in March 2024. The DMA aims to regulate the market power of large digital platforms. An example of a rule proposed by the DMA is the obligation to provide interoperability and data portability. This means that large technology companies, considered “*gatekeepers* companies” under legislation, may be required to allow their services to be interoperable with other competing services and to allow users to take their data with them when switching to another service.

PL 2768/2022 and the DMA have in common the focus on measures to guarantee a more competitive environment, with a view to avoiding abuses arising from economic concentration and, therefore, protecting users' rights (but from a consumerist perspective, distinguishing themselves from the broader focus of PL 2630/2020).

PL 2768/2022 FOR THE PERSPECTIVE OF SOVEREIGNTY: the analysis of PL 2768/2022 also reveals significant dimensions of the debate around digital sovereignty. The highlights are: (i) the promotion of economic self-determination, through measures that ensure a more competitive market and less dependent on decisions made by foreign companies; and (ii) strengthening user rights, applying consumer protection laws.

PL 2338/2023

PL 2338/2023 is one of the bills being processed in the National Congress to regulate Artificial Intelligence. Inspired by the European Union's AI Act, it establishes general rules and obligations for the development and implementation of AI in national territory, seeking to protect fundamental rights and guarantee safer and more reliable systems, through risk classification and management. The project is based on the concept of "human centrality".

PL 2338/2023 FOR THE PERSPECTIVE OF SOVEREIGNTY: PL 2338/2023, like the projects mentioned above, emphasizes a look at digital sovereignty from an individual perspective, removing the focus from the state perspective. At the heart of this project is the notion of user empowerment, mainly through informational sovereignty and self-determination of their data.

In addition to the bills highlighted above, the research also followed the discussions surrounding the formulation of a National Cybersecurity Policy, which resulted in the issuance of Decree n.º 11.856/2024. *This* decree aims to promote the development of national cybersecurity technologies, protect vulnerable groups, combat cybercrime, encourage protection and risk management measures, and strengthen the country's cybersecurity. The National Cybersecurity Committee will be responsible for monitoring the implementation of the National Policy and will be composed of representatives from various bodies and entities.

VI - STRATEGIC DIMENSIONS OF THE DEBATE

The debate on digital sovereignty has gained increasing strength in the current context, and its variables have significant implications for both the present and the future. Let's explore some of these perspectives and the associated challenges.

- **Network fragmentation:** the Internet is global, but local and regional fragmentation has proven to be a major concern shared by different actors, especially with regard to the efforts of different countries and regional blocs seeking to control the flow of data through the imposition of specific regulations. Among the undesirable effects of these processes, implications for interoperability and international collaboration stand out. If this fragmentation intensifies in the future, with different regions adopting divergent approaches to Internet governance, it could have an impact on global cooperation and the resolution of transnational issues.

- **Fragmentation of the user experience:** the user experience varies according to the rules established by the legislation of each country. In some locations, users face restrictions on access to content and services, which can result in restrictions on fundamental rights. Furthermore, this fragmentation can lead to a "tiered" Internet, where different groups of users have different experiences. Among the undesirable effects resulting from these processes, damage to accessibility, freedom of expression and innovation must be considered.

- **Technical and legal challenges:** Digital sovereignty involves technical and legal issues. As technology advances, new challenges emerge. The impact of emerging technologies, such as generative Artificial Intelligence (AI) and 5G, will continue to require innovative approaches and international cooperation. Furthermore, the paradox between legal security and innovation must be matured, so that there is no presupposition of opposition between these two fundamental aspects for the development of the digital economy. For a long time, the digital market and services have developed based on the premise of "*permissionless innovation*". Regulatory policies guided by the idea of digital sovereignty tend to impose stricter market rules. It is necessary to monitor the impacts of these policies on innovation.

- **Governance challenges:** finding a balance between national sovereignty and international cooperation is complex. Multilateral forums continue to play an important role in shaping global governance policies, considering the cross-border

nature of the Internet. Furthermore, attributing regulatory powers over the market and digital services to central state authorities may threaten the participation of different *players* (civil society, academia, technical sector, business sector, etc.) in the process of building public standards and policies if these institutions do not create spaces for consultation and deliberation based on the multisectoral governance model.

FINAL CONSIDERATIONS

The data collected by the research demonstrate that there has been an evident increase in initiatives from different sectors around the topic of digital sovereignty in Brazil in recent years. This debate, which multiplies in the form of academic research, articles, news, legislative projects, civil society articulations, Judiciary decisions, among others, takes place at different levels and involves all sectors of society.

Initiatives and decisions that relate digital sovereignty to digital infrastructures, technologies, data and the Internet demonstrate that there are a variety of interpretations and narratives that coexist linked to the term, and that their practical consequences need to be considered.

The multiplicity of understandings surrounding the concept when it comes to digital technologies and the Internet was mapped and analyzed focusing on the Brazilian situation, but without losing sight of the international agenda on the topic. The difficulty to define the concept is proof of that and illustrates the complexity and diffusion of perspectives, especially because the term can take on different meanings depending on the area in which it is interpreted.

The investigation hypothesis that different existing narratives around digital sovereignty co-produce each other impacts several spheres, including Internet governance. Identifying potential risks linked especially to legislative projects under discussion in the country was highlighted in this study.

However, the analysis presented here, on political, regulatory and technological instruments based on the sovereignty argument, faced the methodological challenge of reaching relevant documents that did not explicitly present the term “digital sovereignty”.

It was observed that the majority of legislative projects do not expressly mention the topic, but reflect aspects related to it, such as the need for its own technological development; local regulation and exercise of jurisdictional power; protection of users’ rights; protection of institutions and the democratic process, among others.

Aware of this limitation, we sought to work with a wide variety of documents and a combination of research tools and discussion spaces to cover as many nuances as possible.

It is also believed that this movement will expand even further considering the number and diversity of existing initiatives linked to the topic, requiring continuous monitoring and the participation of different voices in this debate in order to minimize unwanted risks to society as a whole. The processes and potential practical effects analyzed here can have an impact at the local level and have repercussions on other countries, given Brazil's enormous relevance regarding the regulation of digital media (considering the proportion of its users and experiences such as the Brazil's Internet Bill of Rights and that of the General Data Protection Law.

It is expected that the results of this research can qualify the academic debate and decision-making involving the topic of digital sovereignty from the Brazilian context, exploring its socio-technical dimensions and technological and legal challenges. At the same time, it is seen as an opportunity and relevance to approach future projects considering cross-cutting debates that address, among other factors, the independence of foreign companies, the development of technologies, impacts on the economy and competition, the power of jurisdiction and regulation etc.

REFERENCES

BRASIL. Projeto de Lei nº 2.630/2020. *Institui a Lei Brasileira de Liberdade, Responsabilidade e Transparência na Internet*. Brasília, DF: Câmara dos Deputados, 2022. Availble at: https://www.camara.leg.br/propostas-legislativas/2256735. Accessed at: May 2024.

BELLI, Luca *et. al. Cibersegurança: uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano*. Rio de Janeiro: FGV Direito Rio, 2023. Availble at: https://direitorio.fgv.br/publicacao/ciberseguranca-uma-visao-sistemica-rumo-uma-proposta-de-marco-regulatorio-para-um-brasil Accessed at: May 2024.

CEPI; INTERNET SOCIETY. *Curso Livre "Soberania digital: conceitos, perspectivas e impactos para a Internet no Brasil"*. São Paulo: FGV Direito SP, 2023. Availble at: https://www.isoc.org.br/noticia/disponivel-no-youtube-o-curso-livre-soberania-digital-conceitos-perspectivas-e-impactos-para-a-internet-no-brasil. Accessed at: May 2024.

CERF, Vint G; DRAKE, William J.; KLEINWÄCHTER, Wolfgang. *Internet fragmentation: an overview*. WEF, jan. 2016. Availble at: https://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf. Accessed at: May 2024.

COUTURE, Stephane; TOUPIN, Sophie. *What does the notion of "sovereignty" mean when referring to the digital?* 2019. Availble at: https://journals.sagepub.com/doi/abs/10.1177/1461444819865984 Accessed at: May 2024.

IGF. *Policy Network on Internet Fragmentation*. 2022. Availble at: https://www.intgovforum.org/en/filedepot_download/256/24127 Accessed at: May 2024.

INTERNET SOCIETY. *Navigating digital sovereignty and its impact on the Internet*. Dezembro de 2022. Availble at: https://www.internetsociety.org/wp-content/uploads/2022/11/Digital-Sovereignty.pdf Accessed at: May 2024.

KAUFMAN, Dora. *Democracia e soberania digital*. Época Negócios, 6 out. 2023. Availble at: https://epocanegocios.globo.com/colunas/iagora/coluna/2023/10/democracia-e-soberania-digital.ghtml. Accessed at: May 2024.

LAVITS. *Programa de emergência para a soberania digital*. 18 de agosto de 2022. Availble at: https://lavits.org/programa-de-emergencia-para-a-soberania-digital/ Accessed at: May 2024.

BELLI, Luca *et. al*. *Cibersegurança:* uma visão sistêmica rumo a uma proposta de marco regulatório para um Brasil digitalmente soberano. Rio de Janeiro: FGV Direito Rio, 2023. Availble at: https://direitorio.fgv.br/publicacao/ciberseguranca-uma-visao-sistemica-rumo-uma-proposta-de-marco-regulatorio-para-um-brasil Accessed at: May 2024.

SOUSA, Stenio Santos. *O medo, a incerteza ou qual soberania tecnológica queremos?* Nic.br, 31 ago. 2023. Availble at: https://www.nic.br/noticia/na-midia/o-medo-a-incerteza-ou-qual-soberania-tecnologica-queremos/ Accessed at: May 2024.

STIRLING, Andy. *Keep it complex*. Nature, 22 dez. 2010. Availble at: https://www.nature.com/articles/4681029a Accessed at: May 2024.

ZERBINO, Sofia. *Dossier soberania tecnológica e soberania digital*. *IDDLAC*, n. 6, 31 ago. 2022. Availble at: https://iddlac.org/pt/soberania-tecnologica-e-soberania-digital/ Accessed at: May 2024.

WAGNER, Flávio R. *Aula 2 - Soberania e Internet: Aspectos técnicos, políticos e regulatórios*. YouTube, 17 de novembro de 2023. Availble at: https://www.youtube.com/watch?v=GhJND-qDKj5k&list=PLzm9tGCSV_sIqfVf31iUajw56KKQhpBPp&index=4 Accessed at: May 2024.

APPENDICES

RESEARCH OUTCOMES

In addition to this research report, the project "Digital sovereignty: for what and for whom? Conceptual and political analysis of the concept based on the Brazilian context" included two other main outcomes that deserve to be highlighted and were fed by insights and research data. At the same time, they are a source of information and debates that fed the analyses developed and presented in this report. These products will be detailed below.

Free Course Digital sovereignty: concepts, perspectives and impacts for the Internet in Brazil

The main objective of designing and offering a free course focused on the topic of digital sovereignty was to explore perspectives and debates related to the topic from the Brazilian context and in dialogue with the international agenda. As specific objectives, it was expected that at the end of the course participants would be able to: understand the concept of digital sovereignty and its relationship with other topics on the Internet governance agenda; differentiate perspectives of digital sovereignty and their respective impacts in regulatory terms, on the structure and functioning of the Internet; build a grounded framework around the issue, especially students who work and/or research topics on the Internet governance agenda, in order to enable discussion and qualified decision-making related to digital sovereignty.

The course started on November 6, 2023 and had five meetings. It was carried out online – combining recorded classes, sharing of preparatory readings and live online meetings via the Zoom platform. It was aimed at people from different areas of knowledge and activity, especially those who work with public policies in public, private and civil society organizations. Class diversity was the assumption of the course. Therefore, the application[10] notice for participation considered as selection criteria: sectoral diversity, activity and/or training, regional, gender, color/race/ethnicity, age, in addition to motivation, in order to provide a rich space of exchanges and learning from different perspectives, realities and experiences of the participants. The selection process also considered the justification presented by the candidates regarding the motivation for participation. The course had a total of 61 people selected, of which 37.3%

[10] Notice available at: https://direitosp.fgv.br/sites/default/files/2023-09/edital_curso_livre_soberania_2023_v.2.0.pdf. Accessed in May 2024.

identified themselves as being from academia, 6.6% from the business sector, 16.4% from the government sector, 26.2% from civil society, in addition to counting with the participation of journalists and communication professionals.

All course classes, which totaled more than 7 hours of content and training with experts on the topic, are available on a public playlist on YouTube[11]. Furthermore, participants were encouraged to write an essay on the topic for a digital publication as a product of the course, reflecting reflections and learning from the class. The result of this initiative can also be seen on CEPI FGV Direito SP's Medium12 in a section dedicated to the course.

Internet Impact Brief

The Internet Impact Brief was prepared based on the entire research journey and with the purpose of analyzing the Brazilian bill PL 2630/2020 from the perspective of digital sovereignty. We used the Internet Impact Assessment Toolkit and the Internet Way of Networking framework, both from the Internet Society, as a reference for this analysis. Our objective was to examine how the aforementioned legislative proposal could affect the Internet in its founding characteristics and structures.

The chosen bill has great importance and repercussion today, and was considered paradigmatic for the debate on digital sovereignty.

The enablers “Collaborative development, management and governance”, “Unrestricted accessibility”, “Confidentiality of information data, devices and applications”, “*accountability*” and “Privacy”, which in the methodology developed by the Internet Society are essential for the development of an open, globally connected, secure and reliable Internet, were related to dimensions of sovereignty and discussed based on potential harmful impacts on this structure.

The main risks of the bill discussed in the document lie in the fragmentation of the user experience, vigilantism and threats to collaborative and multistakeholder governance, among others[13].

---

[11] Classes available at: https://www.youtube.com/playlist?list=PLzm9tGCSV_sIqfVf31iU-ajw56KKQhpBPp. Accessed in May 2024.

[12] Publications available at: https://medium.com/o-centro-de-ensino-e-pesquisa-em-inova%C3%A7%C3%A3o-est%C3%A1/soberania/home. Accessed in May 2024.

[13] Publication available at: https://hdl.handle.net/10438/35311

FGV DIREITO SP
CENTRO DE ENSINO
E PESQUISA EM INOVAÇÃO

Internet Society
Capítulo Brasil