INTERNET IMPACT BRIEF

April 2024

Proposals to regulate digital platforms in Brazil: potential impacts for the Internet

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. *Internet Impact Brief.* Proposals to Regulate Digital Platforms in Brazil: Potential Impacts for the Internet. São Paulo: CEPI FGV DIREITO SP; ISOC Brasil, 2024.

LICENCE

Internet impact brief [recurso eletrônico] : proposals to regulate digital platforms in Brazil : potential impacts for the internet / Ana Paula Camelo ... [et al.]. - São Paulo : FGV Direito SP, 2024.
22 p.

Inclui bibliografia.
ISBN: 978-65-87355-57-3

1. Internet. 2. Plataformas digitais. 3. Direito regulatório. I. Camelo, Ana Paula. II. Silveira, Ana Carolina Rodrigues Dias. III. Katano, Beatriz Yuriko Schimitt. IV. Silva, Alexandre Pachedo da. V. Wagner, Flávio Rech. VI. Lana, Pedro de Perdigão. VII. Gatto, Raquel Fortes. VIII. Fundação Getulio Vargas.

CDU 004.738.5

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

INTERNET IMPACT BRIEF

PROPOSALS TO REGULATE DIGITAL PLATFORMS IN BRAZIL: POTENTIAL IMPACTS FOR THE INTERNET

AUTHORS

Ana Carolina Rodrigues Dias Silveira; Ana Paula Camelo; Beatriz Yuriko Schimitt Katano (CEPI FGV Direito SP)

Flávio Rech Wagner; Pedro de Perdigão Lana; Raquel Fortes Gatto (ISOC Brazil)

Version 1.0, April 22, 2024.

ABSTRACT

This Internet Impact Brief analyzes the bill PL 2630/2020 from the standpoint of digital sovereignty using the Internet Impact Assessment Toolkit and the Internet Way of Networking framework, both from the Internet Society, to examine how this Brazilian legislative proposal may affect the Internet in its founding characteristics and structures.

TABLE OF CONTENTS

I – INTRODUCTION

This Internet Impact Brief (IIB) delves into the discussion about the regulation of platforms in the Brazilian context and possible impacts on the structure of the Internet, from the standpoint of digital sovereignty. To this end, Bill n.º 2630/2020 (PL 2630/2020)[i] and the risks that the legal proposal poses to an open, globally connected, secure and trustworthy Internet are analyzed. The initiative of this Impact Brief aims to contribute to the public debate on the topics of digital sovereignty and platform regulation, which have increasingly occupied the political, legislative and academic agendas in recent years in Brazil. Also, the goal is to encourage informed dialogue and contribute to the development and implementation of efficient and accountable instruments within the scope of Internet-related policies. The main risks of the bill discussed in this document lie in the fragmentation of the user experience, vigilantism and threats to collaborative and multisector governance, among others.

II – METHODOLOGY

The analysis of the potential impacts of PL 2630/2020 is based on the application of the critical properties framework [ii] and other elements that constitute the Internet, developed by the Internet Society, and is part of a greater academic effort[1] for mapping and discussion of narratives around the concept of digital sovereignty in Brazil and its developments, exploring its socio-technical, political and legal dimensions regarding the infrastructure and operation of the Internet. To this end, the Internet Impact Assessment Toolkit[iii] is used, to examine how the aforementioned bill could affect the Internet in its founding characteristics and structures.

The enablers "Collaborative development, management and governance", "Unrestricted reachability", "Data confidentiality of information, devices, and applications",

[1] The research project "Digital sovereignty: for what and for whom? Conceptual and political analysis of the concept based on the Brazilian context" is the result of the partnership between ISOC Brazil and the Center for Education and Research on Innovation (CEPI) – FGV Direito SP. To find out more, please access the full research report by clicking here https://bit.ly/cepisoberania. This research mapped the Brazilian legislative production, seeking to identify proposals that connect with the debate on 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. Among the 36 projects mapped and analyzed, the PL 2630/2020 was chosen due to its direct association with the digital sovereignty debate. However, one cannot fail to draw attention to PL 2768/2022, which deals with the regulation of digital platforms, one of the most relevant topics currently in discussions on the exercise of digital sovereignty, given the scope and economic power acquired by *big techs*, in opposition to state power, and also to PL 4723/2020, which determines the preservation of personal data in Brazil and provides other measures.

"Accountability" and "Privacy" were related to dimensions of sovereignty and discussed based on potential harmful impacts on an open, globally connected, secure and trustworthy Internet.

III – CONTEXT

PL 2630/2020

The PL 2630/2020 proposes the regulation of digital platforms in Brazil, establishing rules for content moderation on social networks and messaging services, and changes the platforms' accountability regime.

Comprehensively, this legislative proposal gained prominence due to its focus on content moderation and the responsibility of intermediaries. Through it, the Brazilian Congress aims to create the "Brazilian Law on Freedom, Responsibility and Transparency on the Internet", with the aim of fostering a digital environment that protects citizens and ensures rights. The emphasis on issues related to fighting misinformation and hate speech led PL 2630/2020 to be known as the "Fake News Bill", under the argument of limiting the power of digital platforms and empowering society. Transparency and user control over the moderation of content carried out by platforms stand out as guiding principles of the bill and place the Brazilian debate in a broader context of attempts to regulate the digital environment, also located in other countries.

The bill intends to establish standards and transparency mechanisms for providers of social networks, search tools and instant messaging, as well as guidelines for their use. It also proposes the establishment of a "due process" in relation to content moderation, providing for the guarantee of the right to notification, right to be heard, and broad defense of users. Among its principles, it provides for the protection of constitutional rights to freedom of expression and artistic, intellectual and cultural expression.

The motivation for PL 2630/2020 materializes regulatory pressure that emerges as a reflection of a crisis of trust in networks, driven by the dissemination of hate speech and disinformation, seen as threats to rights and risks to the democratic order. Claims that digital platforms operate in a predatory and harmful manner add to the arguments on the need to act in favor of Brazilian sovereignty.

TABLE 1 – Summary of some of the main aspects in dispute surrounding the PL 2630/2020

Points of greatest consensus	***Most controversial points***
a) Transparency obligations (including periodic reporting and information opening for research); b) Terms and policies in Portuguese and adapted to Brazilian legislation; c) Right to be heard and to full defense in the face of content removal and/or other measures related to content moderation; and d) Promotion of digital education for safe, conscious and responsible use of the Internet.	a) Immunity to political agents, with provisions that inhibit the action from providers; b) Inclusion of provisions on compensation for journalistic and copyright content, issues incorporated from other legislative debates; c) Changing the platform's liability regime; d) Privacy risks; e) Lack of definition regarding institutional arrangements around regulation, inspection and enforcement of the law.

Source: prepared by the authors.

Currently, PL 2630/2020 is 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.

Digital sovereignty inside and outside the Legislature

The relationship between the content of the legislative proposal and the topic of digital sovereignty in a comprehensive way is explicit and central in some debates about the text that is still in progress, emphasizing the "need to have legislation to define very clear parameters and obligations for the operation of these digital platforms in Brazil," and as a way for the country to not depend on or be disproportionately subject to rules established by private companies, according to an assessment by Renata Mielli, coordinator of CGI.br[iv]. The lack of local, Brazilian regulation on the matter is seen as a critical vulnerability, and PL 2630/2020 presents itself as a strategic instrument to deal with the matter based on the country's reality and needs, reinforcing the powers of local authorities in exercising this regulatory control.

It is important to point out that this debate does not take place based on a single, consensual understanding of sovereignty. Different approaches and narratives coexist and are co-produced in the bill debate. In the Brazilian context, it was possible to identify perspectives that coexist and propose (sometimes contradictorily)[2]: (i) increased authority from the State and its institutions; (ii) promotion of a safer and healthier environment; and/or (iii) the ability to guarantee and/or expand citizens' rights. These items, which were also identified in PL 2630/2020 and/or in the narratives linked to it, are detailed in Table 2.

TABLE 2 – Perspectives/goals of digital sovereignty 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;	○ Preservation and/or encouragement of certain local norms and traditions to promote social, cultural and political values from third parties;

[2] Details of local narratives around the concept of digital sovereignty are available in the report from the project research "Digital sovereignty: for what and for whom? Conceptual and political analysis of the concept based on the Brazilian context" https://hdl.handle.net/10438/35312 (2024).

○ Empowerment of citizens and communities to take action and make decisions related to their data and digital activities.	○ 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 "Navigating digital sovereignty and its impact on the Internet" (ISOC, 2022)[v].

In Brazil, the debate on digital sovereignty gained projection in different spaces and contexts, beyond the government sphere. An example of this is the increasing incidence of the topic in multisector forums on Internet governance, such as the Brazilian Internet Forum (FIB), where different voices and standpoints (government, third sector, academic and business community) have reflected on the opportunities and challenges of digital sovereignty in the country[3].

It is also worth highlighting that a Public Consultation was held by the Internet Steering Committee (CGI.br) in 2023 regarding the regulation of digital platforms, with the goal of mapping different types of digital platforms, identifying risks associated with the use of platforms, pointing out regulatory measures capable of mitigating such risks, and also identifying possible actors and paths for regulation[vi] from a multisector debate. Among the guiding axes of the consultation, the "Group of risks – Risks related to threats to digital sovereignty and technological development" stands out, which mobilized debates and contributions around "the country's ability to protect and develop its digital infrastructure autonomously and guarantee the protection of personal and strategic data of its citizens" through (i) State control in relation to the different layers of the digital environment and in relation to national security and data flow; (ii) the development of local technologies, to reduce dependence on foreign companies; (iii) the autonomy and self-determination of individuals, allowing people to make their own decisions about what is done with their information[vii].

As part of legislative activities, hearings [viii] and public debates[ix] were held with experts who addressed, among several issues, the "difficulty in exercising sovereignty due to

[3] It is possible to find submissions of workshops dedicated to digital sovereignty in the Forum about the Internet in Brazil since its 11th edition, which indicates an important increase in the multisector initiative on the subject, which until then was less structured. In 2023, the forum featured two workshops on digital sovereignty, in addition to a main session and a panel during the ISOC Brazil Annual Meeting, not to mention other informal spaces for discussing this topic during the event. The 2024 edition will feature three workshops dedicated exclusively to the topic.

the global nature of the internet", as mentioned in the opinion given in plenary to PL 2630/2020 on April 27, 2023.

No less important, the Digital Sovereignty Charter[x], addressed to Luiz Inácio Lula da Silva, then presidential candidate, and signed by researchers, professors and activists from across the country, also stands out. At the heart of this document was the criticism of the market concentration model represented by big techs and the demand for the development of a national technological infrastructure.

The debate around digital sovereignty is also present in the Judiciary, where many matters related to the operation of the Internet and digital technologies have been discussed (e.g.: accountability of platforms, international data transfer, etc.), which end up affecting the national jurisdiction power. At the Federal Supreme Court, the Declaratory Constitutionality Action n.º 51[xi] 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). Other highlights are the extraordinary appeals[4] that discuss the constitutionality of art. 195 from the Brazil's Internet Bill of Rights (MCI, Law n.º 12.965/2014[xii]) and the need for intervention by the Judiciary as a requirement for holding application providers responsible for content generated by users (still under trial).

The Supreme Electoral Court has also been involved in this debate, through measures that seek to protect the electoral process from threats posed by the misuse of networks, a central issue in the debate about the regulation of 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.

[4] Namely, Extraordinary Appeal n.º 1037396/SP and Extraordinary Appeal n.º 1057258/MG.

[5] 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.

IV – ANALYSIS OF THE IMPACT OF PL 2630/2020 ON THE FUNDAMENTAL PROPERTIES OF THE INTERNET FROM THE STANDPOINT OF DIGITAL SOVEREIGNTY

This section analyzes the legislative project that is the subject of this report aiming at understanding how it could impact the properties and other constituent elements of the Internet Way of Networking (IWN), under the lens of sovereignty digital.

The IWN is a model proposed by the Internet Society to describe what makes the Internet "the Internet"[xiii], not only as a complex, diverse and dynamic network, but also as an open, globally connected, secure and trustworthy network. This model is defined by a set of "critical properties" and "enabler elements" that support the growth and adaptability of the "network of networks".[xiv].

The analysis based on the most recent public versions of PL 2630/2020, through the lens of digital sovereignty, identified possible impacts on critical properties and some enabler elements, as described below.

Critical properties

According to the IWN framework, the Internet's network mode is made up of five critical properties necessary for the structure and operation of the Internet. They are: (1) an accessible infrastructure with a common protocol; (2) an open architecture of interoperable and reusable building blocks; (3) decentralized management and a single distributed routing system; (4) common global identifiers; and (5) a technology-neutral, general-purpose network.

For the purposes of this Impact Brief, no impacts on critical properties were identified based on this analysis. Special attention was paid to the impacts on enablers that support an open, globally connected, secure and trustworthy Internet.

Enablers of an open, globally connected, secure and trustworthy Internet

The enablers[xv] can work as tools for analyzing the potential effects that certain legislative changes may entail, ultimately affecting the desired goals.

For the purposes of this Impact Brief, potential impacts of PL 2630/2020 were identified on the enablers described in Table 3 and detailed below.

TABLE 3 – Analytical summary: PL 2630/2020, enablers and perspectives for sovereignty

Goal	*Enabler*	*Perspectives of sovereignty*	*Impacts*
Open Internet	Collaborative development, management and governance	National security and ability to enforce laws: governments that want to control how Internet operations and resources are run (i.e., regulatory power).	- Institutional structure of regulation, control and supervision - Centralization of governance - Threat to the multisector governance model
Globally connected internet	Unrestricted reachability	National security and ability to enforce laws: governments that want to control how Internet operations and resources are run (i.e., regulatory power/jurisdiction).	- Local regulation (specific content moderation rules and other obligations) - Risk of fragmentation of the "user experience"
Secure Internet	Data confidentiality of information, devices and applications	National security and ability to enforce laws: (i) governments that want to control how Internet operations and resources are run; (ii) increase State power and access to data (i.e., jurisdiction power).	- State sovereignty x individual sovereignty (informational sovereignty + data self-determination) - Security
Trustworthy Internet	Accountability	Protection of rights and empowerment of citizens/users and communities: autonomy of citizens over their interactions with devices, platforms and the way they manage their data.	- Autonomy in decision making - Digital human rights - Freedom of expression in the digital space, especially in relation to control of their data
	Privacy	Protection of rights and empowerment of citizens/users and communities: autonomy of citizens over their interactions with devices, platforms and the way they manage their data.	- Autonomy in decision making - Data control - Human rights in the digital world - Privacy

			- Freedom of expression in the digital space, especially in relation to control of their data

Source: based on "Contribuição do capítulo brasileiro da *Internet Society* ao processo de desenvolvimento de política 'Habilitadores de uma Internet aberta, globalmente conectada, segura e confiável'" (ISOC Brazil)

Support for an open Internet: Collaborative development, management, and governance

The analysis of the Internet development, management and governance from a collaborative standpoint, essential characteristics of support for an open Internet, allows us to identify in PL 2630/2020 one of the dimensions of digital sovereignty: the State's ability to enforce its own laws, which directly relates to the issue of jurisdiction. The debate surrounding the institutional structure responsible for enforcing the law could have a significant impact on the Internet governance model in Brazil.

Historically, Brazil has adopted a multisector model of Internet governance. As in many other countries, there was a separation between the regulation of telecommunications operators and the regulation of the Internet (please refer to ANATEL rule 04/95 and art. 61 of the General Telecommunications Law – Law n.º 9.472/97). The Internet Steering Committee (CGI.br) was also created in this context, with representatives from different sectors in its composition (public sector, business sector, third sector and scientific and technological community). Since then, a logic that privileges the ideas of "permissionless innovation"[6] and self-regulation[7] has been in force. However, there has been growing pressure to regulate application providers, given the negative externalities caused especially by social networks (such as the dissemination of misinformation and hate speech).

[6] The principle of "permissionless innovation" has been one of the foundations for the development of an open Internet. It presumes the ability to create new things without prior authorization or license, which has allowed the rapid evolution of Internet applications over the last few decades, through a wide variety of business models.

[7] In line with the principle of "permissionless innovation," for a long time there was an understanding that "self-regulation" by companies in the sector, through their corporate governance structures, would be sufficient for the good development and use of the Internet. However, state regulation has become increasingly present, considering the potential impacts on society, the need to develop public policies to manage these impacts, and the conflicts of interests between public (social) and private (corporate). The challenge is to understand what the limits of this regulation should be and what the undesirable effects could be.

Regulation is a way for countries to exercise digital sovereignty. Many governments face difficulties exercising authority over digital assets and services that operate or are made available locally – often through foreign multinational companies – and want to reassert their ability to define and enforce laws within their territory.[xvi]. With the regulatory proposals, the discussion around the creation of an institutional architecture that plays the role of control and supervision also arises.

PL 2630/2020 still lacks a definition regarding the institutional structure to promote regulation (i.e., the establishment of guidelines, norms, technical standards, etc.) and supervision of the enforcement of the norm. On the eve of the vote, in April 2023, the rapporteur removed the figure of the so-called "Autonomous Supervision Entity" from the legislative proposal. This lack of definition causes legal uncertainty, also because there are several provisions of the bill that will depend on subsequent regulation and, depending on how it is done, there may or may not be negative impacts on the structure of the Internet. Ultimately, these legislative omissions could be judicialized, leaving judges to decide at their own discretion, a risk that is amplified given the enormous volume of content subject to moderation on a daily basis.

One of the proposals to fill the aforementioned institutional gap would be to delegate these powers to a central state authority, such as the National Telecommunications Agency (ANATEL), which has already been incorporated into other bills. ANATEL is the Brazilian federal agency responsible for regulating and supervising the telecommunications sector in the country. Some models have been discussed in this sense, in parallel with the processing of PL 2630/2020. This is the case, for example, of PL 2768/2022, which proposes a regulatory approach focused on economic aspects, emptying the debate around content moderation.

PL 2768/2022[xvii] also gives ANATEL powers to act on matters of a competitive nature. Currently, this role is exclusively the responsibility of the Administrative Council for Economic Defense (CADE), which has maintained an understanding of the prevalence of consumer well-being, avoiding acting against market concentration.

The possible delegation of regulatory powers to a central authority, linked to the State, requires some care. Among the points of attention, the following stand out: (i) the challenge of managing conflicts of interest between different actors and players in the market; (ii) the preservation of the multisector governance model, through the participation of representatives from the different sectors involved in decision-making; and (iii) in-

terdisciplinary technical competence, especially considering the challenge of regulating and supervising content moderation, a central issue of PL 2630/2020 and the regulatory debate surrounding the responsibility of platforms in Brazil[8].

Support for a globally connected Internet: Unrestricted reachability

PL 2630/2020 can generate impacts on unrestricted reachability, essential for achieving the goal of a globally connected Internet, in terms of two possible developments of the concept of digital sovereignty: (i) the power to enforce its laws and (ii) the issue of sovereignty related to jurisdiction. Both aspects concern the notion of digital sovereignty related to the State's point of view.

Like European legislation, PL 2630/2020 establishes very specific rules for digital application providers who wish to carry out their activities in Brazil. The goal of such mechanisms is to defend Brazilian interests, through means of protection and empowerment of local norms and institutions, thus reinforcing their regulatory power. However, one cannot fail to consider that an excess of local regulatory instruments can create an obstacle to the operation of the globally connected Internet.

Legislation such as that proposed by PL 2630/2020 raises questions about the risks of Internet fragmentation, especially the "fragmentation of user experience", given the conflict of rules between different jurisdictions. This is because specificities in the legislation that regulates a given topic can lead to a dissonance between the laws of the country in which the company is headquartered, generally States in the Global North, and national laws, which in turn can result in the impossibility of carrying out certain operations, generating losses and insecurity for users.

Establishing standards for the operations of foreign companies on national soil can be one of these objects of conflict related to the idea of jurisdiction and the power to regulate topics already covered by Brazilian legislation, as set out in art. 3rd, XIII (adaptation to Brazilian legislative diplomas), in art. 11 (exhaustive list of illicit conducts subject to moderation), and in art. 41 (imposition of operational operating rules on instant messaging services). Furthermore, entry barriers may be being created for other stakeholders, which may concentrate niche activities in a small number of players already established in the sector.

[8] This task should ideally be shared with different bodies, as occurs with the control exerted over other media. This model brings more security in relation to the protection of freedom of expression.

Support for a secure Internet: Data confidentiality of information, devices and applications

Regarding the dimension of confidentiality, an essential requirement for a secure Internet, it is possible to identify that PL 2630/2020 may generate impacts on three aspects of digital sovereignty: (i) the issue of national security; (ii) the State's ability to enforce its own laws, which is directly related to the issue of jurisdiction; and (iii) the right to self-determination of user data, a sphere of digital sovereignty focused on the individual aspect. It is extremely important to consider item (iii), which, to a certain extent, competes with items (i) and (ii), focused on digital sovereignty related to the interests of the State, while the third item prioritizes the protection of citizens' rights.

The art. 45 of PL 2630/2020 obliges platforms to notify to the authorities that they suspect that a crime against life has occurred or may occur. Art. 46 obliges them to store, for a period of six months, removed or deactivated content – depending on compliance with the moderation rules introduced by law –, as well as data and metadata related to this content. There is no consideration of possible technical limits to fulfilling these obligations, for example, in the case of messaging services based on encryption[9]. This creates great insecurity for users.

It is worth mentioning that, in this case, there is a conflict between the State's power to regulate, which aims to overlap its jurisdiction over foreign companies that intend to operate in Brazil, and the individual rights of service users. Citizens, when using digital applications, want the services to be secure and to be able to send messages without running the risk of them being accessed by individuals external to the topic. It is important to highlight that, although there is a similarity between the themes of confidentiality and privacy, they are different concepts. While privacy relates much more to protecting users' data and their ability to decide how it will be handled, confidentiality refers to the possibility of users sending messages with security mechanisms, such as encryption, so that third parties cannot have access to the content or whoever is sending it[xviii]. It is worth highlighting that both (privacy and confidentiality – "or secrecy of communications") are guaranteed by the MCI (please refer to art. 11). It is understood that the possibility of monitoring content by third parties represents one of the main risks to confidentiality, in addition to risks to user safety, and must be studied with caution so that it is possible to define limits to the application of this device, under penalty of generating a excessive vigilantism that reduces citizens' freedom.

[9] There are two ongoing actions at the Supreme Court (ADPF 403 and ADI 5527) that analyze end-to-end encryption and its implications from a legal standpoint. The rapporteurs of both actions have already stated that encryption is a necessary tool for the protection of fundamental rights.

The art. 46, in turn, proves problematic as it stipulates that content removed from digital platforms be maintained so that it can be used in future analyses. This contradicts the Brazilian General Data Protection Act (LGPD – Law n.º 13.709/2018), which defends minimum data retention. Keeping a record of content longer than necessary increases the risk of breaching confidentiality, which also increases the risk of undue exposure of content to third parties.

Support for a trustworthy Internet: Accountability

Regarding the dimension of support for a secure Internet based on the issue of accountability, two dimensions of the debate on sovereignty are identified: (i) exercise of the power of regulation and jurisdiction with regard to compliance with local laws and (ii) guarantee of the exercise and protection of rights.

The emphasis on the transparency of content moderation practices posted by third parties on social networks and the adoption of mechanisms and tools for information about content made available to the user, in turn, is based on the protection of the end user and their rights, in accordance with the Brazilian legal system and due legal process.

PL 2630/2020 establishes a series of obligations that may have impacts on this enabler, which include: (i) rules and obligations concerning transparency, which include the provision of biannual reports with qualitative and quantitative information about the content moderation procedures provided for in the law; (ii) the adoption of terms of use and policies in Portuguese and in compliance with local legislation/reality; (iii) the institution of “due process” (right to notification, right to dispute and defense); and (iv) carrying out annual external audits.

The bill also provides for some mandatory information, such as indicative age range, prohibited content, moderation rules, and forms of notification about possible irregularities. The user who has their content and/or account removed, for example, must be notified about the nature of the measure adopted and its territory of application and the foundation of the decision based on the indication of the terms of use violated, giving them the opportunity to right to contest and defend, to reverse the measure.

The mandatory external audits, on the other hand, must also cover some aspects provided for by law, such as efficiency in the adoption of measures and identification of systemic risks; assessment of discriminatory treatment and/or bias in decisions during content/account moderation; impact of algorithms on content distribution etc.

However, it is possible to identify, linked to these measures, risks to freedom of expression and the human rights of users that go beyond the dimension of transparency and that intersect, in turn, with discussions and impacts regarding security, protection of privacy and confidentiality.

In this sense, an intersection is identified between ideas of "state sovereignty" and "individual sovereignty" with regard to decision-making power and authority. On the one hand there are rules in favor of the collectiveness and the need to obtain/guarantee security, justice, peace, and well-being for citizens; on the other hand, the autonomy of individuals to take responsibility for their own decisions and lives, which would be possible through notification instruments and linguistic empowerment in relation to the platforms' terms of use and policies.

Support for a trustworthy Internet: Privacy

In terms of privacy, which supports a trustworthy Internet, three developments of the concept of digital sovereignty that impact the discussion can be identified: (i) exercise of the power of jurisdiction; (ii) informational sovereignty; and (iii) data self-determination. It is noteworthy that item (i) is focused on the notion of sovereignty related to the State, while (ii) and (iii) prioritize the sphere of users' interests.

The obligations brought by art. 42, 45 and 46 from PL 2630/2020, by bringing a risk to data confidentiality (as mentioned in a previous topic), also put users' privacy at risk, both by monitoring shared content – including in encrypted private messages – and for storing an immense volume of personal data, including possibly sensitive data. Any leakage of this data would compromise users' privacy.

These obligations serve the purpose of facilitating the exercise of the power of local jurisdiction (again, a form of manifestation of digital sovereignty), through the provision of data that can assist investigations. However, here once again we identify the conflict between the notion of "state sovereignty" (i.e., power of jurisdiction) and the notion of "individual sovereignty", which involves the informational sovereignty of users and the self-determination of their data. This perspective of individual rights is supported by the General Data Protection Act, which establishes the principle of "need", according to which the processing of personal data (which includes collection and storage, among other operations) must be restricted to the "minimum necessary " to achieve the purposes of the service, "encompassing pertinent, proportional and not excessive data" (please refer to art. 6th, III, of the LGPD). Furthermore, the MCI provides for the confidentiality of communications between users (refer to art. 11), except for the mandatory storage, for legal purposes, of only the connection data.

Although PL 2630/2020 brings privacy and protection of users' personal data as one of its principles, making several references to the LGPD[xix], the devices mentioned above represent important warning points.

It is worth noting that issues related to privacy are closely linked to the analyses of other topics in this IIB. It is not possible to conceive an accountability and governance model that does not protect the privacy of users and the confidentiality of their communications on the Internet.

V – FINAL REMARKS AND RECOMMENDATIONS

In July 2020, Brazil began discussing standards and transparency mechanisms for providers of social networks, search tools and instant messaging, as well as guidelines for their use, based on the presentation of the legislative proposal for the "Brazilian Law on Freedom, Responsibility and Transparency on the Internet" (PL 2630/2020). One of the main goals of the bill is to regulate the duties and responsibilities of intermediaries in the Brazilian context.

This report used the Internet Impact Assessment Toolkit to assess how this bill could affect the global Internet through the lens of the digital sovereignty debate. To this end, the latest version of PL 2630/2020 (presented in the plenary of the House of Representatives on April 27th, 2023) available until the finalization of this document was considered.

From this analysis, no direct and immediate impacts were identified on the critical properties that support the Internet infrastructure. However, it is discussed how PL 2630/2020 may affect enablers that allow the Internet to operate and prosper as an open, globally connected, secure and trustworthy resource for everyone. The discussion was established based on arguments and dimensions of digital sovereignty that can cause harm or reduce: (i) collaborative development and governance; (ii) unrestricted reachability; (iii) the confidentiality of information, devices and applications; (iv) accountability; and (v) privacy.

Despite the proposal's significant technical and legal advances in relation to the version approved by the Senate, some points of attention were identified, which could have consequences for innovation, resilience and fragmentation of the Internet, highlighting the relevance of the debate.

It is recommended to pay attention to these possible impacts, aiming at a legislation that is adequate to face the challenges generated by the misuse of social networks

and the negative externalities of the business models adopted by the platforms, but which is also capable of following the dynamism of transformations generated by technological evolution.

REFERENCES

[i] 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. Available at: https://www.camara.leg.br/propostas-legislativas/2256735. Accessed at: April 2024.

[ii] ISOC BRASIL. *O Modo Internet de Interconectividade*: um fundamento para o sucesso. [S.d.]. Available at: https://www.isoc.org.br/files/IWN_introducao_traducao%20(1).pdf. Accessed at: April 2024.

[iii] INTERNET SOCIETY. *Internet Impact Assessment Toolkit*. [no date]. Available at: https://www.Internetsociety.org/issues/Internet-way-of-networking/Internet-impact-assessment-toolkit/ Accessed at: April 2024.

[iv] TOCH, Lucas. "Regulação promove Internet mais saudável para a democracia", diz Renata Mielli (2023). *NIC.br*, Jan 2, 2024. Available at: https://www.nic.br/noticia/na-midia/regulacao-promove-Internet-mais-saudavel-para-a-democracia-diz-renata-mielli/. Accessed at: April 2024.

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 at: April 2024.

[vi] NIC.br. Grupo de Trabalho sobre Regulação de Plataformas do CGI.br. *Sistematização das contribuições à consulta sobre regulação de plataformas digitais.* São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2023. p. 22. Available at: https://cgi.br/media/docs/publicacoes/1/20240227162808/sistematizacao_consulta_regulacao_plataformas.pdf. Accessed at: April 2024.

[vii] NIC.br. Grupo de Trabalho sobre Regulação de Plataformas do CGI.br. *Sistematização das contribuições à consulta sobre regulação de plataformas digitais.* São Paulo: Núcleo de Informação e Coordenação do Ponto BR, 2023. p. 16. Available at: https://cgi.br/media/docs/publicacoes/1/20240227162808/sistematizacao_consulta_regulacao_plataformas.pdf Accessed at: April 2024.

[viii] APERFEIÇOAMENTO LEGISLAÇÃO BRASILEIRA – Internet – Tecnologia e soberania nacional, 31/08/2021 (1h43min). Publicado pelo canal Câmara dos Deputados. Available at: https://www.youtube.com/watch?v=_L_F1xYbNRc. Accessed at: April 2024.

[ix] CICLO DE DEBATES PÚBLICOS: Lei de Combate às Fake News (PL 2630/20), 29/07/2020 (2h12min). Publicado pelo canal Câmara dos Deputados. Available at: https://www.youtube.com/watch?v=iWB97_-GYu4. Accessed at: April 2024.

[x] CARTA SOBERANIA DIGITAL. [S.d.]. Available at: https://cartasoberaniadigital.lablivre.wiki.br/carta/. Accessed at: April 2024.

[xi] STF. *Autoridades nacionais podem requisitar dados diretamente a provedores no exterior, decide STF.* 23 de fevereiro de 2023. Available at: https://portal.stf.jus.br/noticias/verNoticiaDetalhe.asp?idConteudo=502922&ori=1. Accessed at: April 2024.

[xii] BRASIL. *Lei nº 12.965, de 23 de abril de 2014*. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF, 23 abr. 2014. Available at: http://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm. Accessed at: April 2024.

[xiii] ISOC BRASIL. *O Modo Internet de Interconectividade*: um fundamento para o sucesso. [S.d.]. Available at: https://www.isoc.org.br/files/IWN_introducao_traducao%20(1).pdf. Accessed at: April 2024.

[xiv] ISOC. *How to conduct an Internet Impact Brief*. Internet Impact Assessment Toolkit, 2021. p. 3. Available at: https://www.Internetsociety.org/resources/doc/2021/how-to-conduct-an-Internet-impact-brief/. Accessed at: April 2024.

[xv] ISOC Brazil. *Contribuição do Capítulo Brasileiro da Internet Society ao processo de desenvolvimento de política "Habilitadores de uma Internet aberta, globalmente conectada, segura e confiável".* [202-]. Available at: https://isoc.org.br//files/Contribui%C3%A7%C3%A3o%20do%20Cap%C3%ADtulo%20Brasileiro%20da%20Internet%20Society%20ao%20Processo%20de%20Desenvolvimento%20de%20Pol%C3%ADtica%20%E2%80%9CHabilitadores%20De%20Uma%20Internet%20Aberta,%20Globalmente%20Conectada,%20Segura%20E%20Confi%C3%A1vel%E2%80%9D.pdf. Accessed at: April 2024.

[xvi] INTERNET SOCIETY. *Navigating digital sovereignty and its impact on the Internet*. December 2022. p. 12. Available at: https://www.Internetsociety.org/wp-content/uploads/2022/11/Digital-Sovereignty.pdf. Accessed at: April 2024.

[xvii] BRASIL. *Projeto de Lei nº 2.768/2022*. Dispõe sobre a organização, o funcionamento e a operação das plataformas digitais que oferecem serviços ao público brasileiro e dá outras providências. Brasília, DF: Câmara dos Deputados, 2022. Available at: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2337417. Accessed at: April 2024.

[xviii] INTERNET SOCIETY. *Navigating digital sovereignty and its impact on the Internet*. December 2022. p. 33. Available at: https://www.Internetsociety.org/wp-content/uploads/2022/11/Digital-Sovereignty.pdf. Accessed at: April 2024.

[xix] BRASIL. *Lei nº 13.709, de 14 de agosto de 2018*. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF, 2018. Available at: www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Accessed at: April 2024.

FGV DIREITO SP
CENTRO DE ENSINO
E PESQUISA EM INOVAÇÃO

Internet Society
Capítulo Brasil