Internet Impact Brief

Proposals to Regulate Digital Platforms In Brazil: Potential Impacts on the Internet

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 (Internet Society Brazil Chapter)

December 2024

Abstract

This Internet Impact Brief analyzes Bill 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.

1. Introduction

This Internet Impact Brief (IIB) explores the debate on platform regulation in the Brazilian context and its potential effects on the Internet's fundamental characteristics, focusing on digital sovereignty. It examines Bill No. 2630/2020 (Bill 2630/2020) and the risks it poses to an open, globally connected, secure, and trustworthy Internet. The goal is to contribute to the public debate on digital sovereignty and platform regulation, topics increasingly prominent in Brazil's political, legislative, and academic agendas. The IIB also aims to foster informed dialogue and support the development of effective, accountable Internet policies. Key risks of the bill include user experience fragmentation, increased surveillance, and threats to collaborative, multistakeholder governance.

2. Context

Bill 2630/2020 proposes regulating digital platforms in Brazil[1], establishing rules for content moderation on social networks and messaging services, and changing platforms' accountability regimes. This legislative proposal gained prominence for its focus on content moderation and intermediary responsibility. Nicknamed the “Fake News Bill”, it aims to combat misinformation and hate speech

1 For a comprehensive understanding of the Brazilian context surrounding the discussion of Bill 2630, please visit https://bit.ly/IIB2630br

(viewed as threats to rights and democratic order) by limiting digital platforms' power and, at the same time, empowering society. Transparency and user control over content moderation by platforms are central principles, situating the Brazilian debate within broader global regulatory efforts. Claims that digital platforms act in a predatory and harmful way strengthen arguments for Brazilian sovereignty.

In December 2024, discussions around Bill 2630/2020 are inactive, and there is no prediction of when or if they will resurface. However, several controversial aspects remain. In April 2024, the House President announced a working group to discuss the matter, creating uncertainty about the agenda's future. The absence of Brazilian regulation on this issue is seen as a critical vulnerability. Bill 2630/2020 aims to address this gap, tailoring solutions to the country's context and reinforcing local authorities' powers to exercise regulatory control.

3. Methodology

The analysis of the potential impacts of Bill 2630/2020 is based on the application of the critical properties' framework and other elements that constitute the Internet, developed by the Internet Society, and is part of a greater academic effort[2] 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 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," "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.

2 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 Bill 2630/2020 was chosen due to its direct association with the digital sovereignty debate. However, one cannot fail to draw attention to Bill 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 Bill 4723/2020, which determines the preservation of personal data in Brazil and provides other measures.

4. Analysis of the Impact of Bill 2630/2020 on the Fundamental Properties of the Internet from the Standpoint of Digital Sovereignty

This section analyzes the impact of Bill 2630/2020 on the critical properties and enablers as defined by the Internet Way of Networking (IWN) framework through the lens of digital sovereignty, based on the most recent public versions of the bill, as outlined below.

Critical Properties

According to the IWN framework, the Internet's networking 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.

No impacts on critical properties were identified for the purposes of this impact brief. Special attention was thus 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 can work as tools for analyzing the potential effects that certain legislative changes may entail, ultimately affecting the desired goals. Potential impacts of Bill 2630/2020 were identified on five enablers, as described in Table 1 and detailed below.

TABLE 1 – Analytical summary: Bill 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 versus individual autonomy and self-determination. (informational sovereignty and 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

Support For an Open Internet: Collaborative Development, Management, and Governance

The analysis of the Internet development, management, and governance from a collaborative standpoint, essential for supporting an open Internet, allows us to identify in Bill 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 on 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 multistakeholder 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. The Brazilian Internet Steering Committee (CGI.br) was also created in this context, with representatives from different sectors in its composition (public sector, business sector, NGOs, and scientific and technological community). Since then, the ideas of "permissionless innovation"[3] and self-regulation[4] have 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).

Many governments struggle to exercise authority over digital assets and services operating locally—often through foreign multinational companies—and seek to reassert their ability to define and enforce laws within their territory. Regulation serves as a means for countries to assert digital sovereignty. Regulatory proposals also prompt discussions about creating an institutional framework for control and supervision.

Bill 2630/2020 lacks a clear definition of the institutional structure responsible for promoting regulation (e.g., guidelines, norms, technical standards) and supervising the norm's enforcement. This uncertainty creates legal risks, as many provisions of the bill depend on subsequent regulation. Depending on its implementation, there could be negative impacts on the Internet's structure. Legislative gaps might lead to judicialization, leaving judges to decide at their discretion—a risk amplified by the vast volume of content requiring daily moderation.

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

3 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.
4 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.

supervising the telecommunications sector in the country. The proposal of granting ANATEL this role has faced many controversies, as there is a legal separation in Brazil among the telecommunications and Internet sectors. Some alternative models have been discussed in parallel with the processing of Bill 2630/2020. This is the case, for example, of Bill 2768/2022, which proposes a regulatory approach focused on economic aspects.

Bill 2768/2022 also grants ANATEL powers to address competitive matters, a role currently exclusive to the Administrative Council for Economic Defense (CADE). CADE has prioritized consumer well-being in its approach, refraining from acting against market concentration.

The possible delegation of regulatory powers to a central authority linked to the State requires careful consideration.

Key points of attention include: (i) managing conflicts of interest among different market actors and players; (ii) preserving the multistakeholder governance model by ensuring participation from various sectors in decision-making; and (iii) ensuring interdisciplinary technical competence, particularly given the challenges of regulating and supervising content moderation—a central issue in Bill 2630/2020 and the broader regulatory debate on platform responsibility in Brazil[5].

Support for a Globally Connected Internet: Unrestricted Reachability

Bill 2630/2020 can generate impacts on unrestricted reachability, essential for achieving the goal of a globally connected Internet, in terms of two possible dimensions 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, Bill 2630/2020 establishes specific rules for digital application providers operating in Brazil, aiming to protect Brazilian interests by empowering local norms and institutions and reinforcing regulatory power. However, excessive local regulations could hinder the operation of the globally connected Internet.

Legislation like Bill 2630/2020 raises concerns about Internet fragmentation, particularly "fragmentation of user experience," due to conflicting rules across jurisdictions. Differences between national laws and those of companies' home countries, typically in the Global North, can lead to operational challenges, user losses, and insecurity.

Establishing standards for the operation of foreign companies on national territory can be one of these objects of conflict related to the idea of jurisdiction and the power to regulate topics already covered

5 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.

by Brazilian legislation, as set out in Bill 2630, in Article 3, XIII (adaptation to Brazilian legislative diplomas), in Article 11 (exhaustive list of illicit conducts subject to moderation), and in Article 41 (imposition of operational operating rules on instant messaging services). Furthermore, entry barriers may be created for other stakeholders, which may concentrate niche activities in a small number of players already established in the sector.

Support for a Secure Internet: Data Confidentiality of Information, Devices, and Applications

Regarding the dimension of confidentiality, an essential requirement for a secure Internet, Bill 2630/2020 may generate impacts on three dimensions of digital sovereignty: (i) the issue of national security; (ii) the State's ability to enforce its own laws, which is directly related to 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.

Article 45 of Bill 2630/2020 obliges platforms to notify the authorities that they suspect that a crime against life has occurred or may occur. Article 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.

Article 45 of Bill 2630/2020 requires platforms to notify authorities if they suspect a crime against life has occurred or might occur. Article 46 mandates platforms to store removed or deactivated content, along with related data and metadata, for six months. This applies when such content is taken down in compliance with the moderation rules introduced by the law. There is no consideration of possible technical limits to fulfilling these obligations, for example, in the case of messaging services based on encryption[6], as these services are also covered by the bill This may create great insecurity for users, as they may lose trust that their communications are kept confidential.

It is worth mentioning that, in this case, there is a conflict between the State's power to regulate, which aims to extend 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 the risk of being accessed by external actors.

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

6 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.

messages with security mechanisms, such as encryption, so that third parties cannot have access to the content or whoever is sending it[7]. It is worth highlighting that both (privacy and confidentiality – "or secrecy of communications") are guaranteed by the Brazilian Internet Bill of Rights - "Marco Civil da Internet" (please refer to the Bill's Article 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 provision, under great risk of generating excessive vigilantism that reduces citizens' freedom.

Article 46 conflicts with the Brazilian General Data Protection Act (LGPD – Law No. 13.709/2018), which emphasizes minimal data retention. Keeping content longer than necessary heightens the risk of confidentiality breaches and undue exposure to third parties.

Support for a Trustworthy Internet: Accountability

Regarding the support for a trustworthy Internet based on 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.

Bill 2630/2020 emphasizes transparency in 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. This aims to protect the end user and their rights in accordance with the Brazilian legal system and due legal process.

Bill 2630/2020 establishes various obligations that may affect this enabler, including: (i) transparency rules, such as biannual reports with qualitative and quantitative information on content moderation; (ii) adoption of terms of use and policies in Portuguese, aligned with local legislation; (iii) institution of "due process" rights (notification, dispute, and defense); and (iv) annual external audits.

The bill mandates the provision of certain information, including indicative age range, prohibited content, moderation rules, and notification procedures for reporting irregularities. For instance, users whose content or accounts are removed must be informed of the nature of the measure, its jurisdictional scope, and the specific terms of use violated. They must also have the opportunity to contest the decision and seek its reversal. Mandatory external audits must address aspects such as the efficiency of measures, identification of systemic risks, evaluation of discriminatory treatment or bias in moderation decisions, and the impact of algorithms on content distribution. However, these measures

7 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.

raise concerns about risks to freedom of expression and users' human rights, extending beyond transparency to issues of security, privacy, and confidentiality.

This highlights an intersection between state sovereignty and individual autonomy in decision-making authority. On one side, there are rules promoting collective interests, such as security, justice, and well-being; on the other, individual autonomy emphasizes self-determination and responsibility, supported by notification mechanisms and linguistic empowerment regarding platform policies.

Support for a Trustworthy Internet: Privacy

In terms of privacy, which supports a trustworthy Internet, three dimensions of digital sovereignty 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 outlined in Articles 42, 45, and 46 of Bill 2630/2020, which pose risks to data confidentiality (as previously discussed), also endanger users' privacy. This is due to the monitoring of shared content, including encrypted private messages, and the storage of vast amounts of personal, potentially sensitive, data. Any data breach would severely 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 autonomy and self-determination," which involves the informational sovereignty of users and the self-determination of their data. This perspective of individual rights is supported by the Brazilian General Data Protection Act (LGPD), which establishes the principle of "necessity" (aiming at data minimization), 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 Article 6th, III, of the LGPD). Furthermore, the Brazilian Internet Bill of Rights provides for the confidentiality of communications between users (refer to the Bill's Article 11), except for the mandatory storage, for legal purposes, of only the connection data.

Although Bill 2630/2020 recognizes privacy and data protection as guiding principles, with several references to the LGPD[8]. These provisions raise significant concerns. Finally, privacy is deeply

8 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.

interconnected with other issues analyzed in this IIB. A robust accountability and governance model for the Internet must safeguard users' privacy and the confidentiality of their communications.

5. 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" (Bill 2630/2020). One of the main goals of the bill is to regulate the duties and responsibilities of intermediaries in the Brazilian context.

This Internet Impact Brief 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 Bill 2630/2020 (presented in the plenary of the House of Representatives on 27 April 2023) is considered until the finalization of this document. From this analysis, no direct and immediate impacts were identified on the critical properties that support the Internet infrastructure.

However, it is discussed how Bill 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 highlighted dimensions of digital sovereignty that could undermine or reduce: (i) collaborative development and governance; (ii) unrestricted reachability; (iii) information, device, and application confidentiality; (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 that these potential impacts be carefully addressed. Legislation should strive to effectively address the challenges posed by the misuse of social networks and the externalities of platform business models. At the same time, the rule of law should remain adaptable to the dynamic changes driven by technological evolution.