March 2026

Internet Impact Brief

PL 4752/2025

Internet Society
Capítulo Brasil

Coordination

Grupo de Trabalho de Criptografia - ISOC Brasil

IP.Rec

Reviewers

Flávio Rech Wagner

Laura Pereira

Raquel Fortes Gatto

João Moreno Falcão

Pedro Amaral

Support

ISOC Foundation

This Internet Impact Brief is an outcome of the project Encryption and Digital Rights in Brazil: Capacity Building, Dialogue, and Policy Advocacy.

Table of Contents

Executive Summary

PL 4752/2025 represents a significant advance in Brazilian cybersecurity governance, with a mixed impact on the Internet's architecture:

Category	Description	Impact
Type of Change	National legislation establishing a cybersecurity governance framework	Regulatory
Scope	Federal public administration; voluntary private-sector participation	National
Critical Properties	4 of 5 properties potentially affected	Low
Enablers	7 of 10 enablers impacted (4 positively, 3 with mixed/negative effects)	Mixed
Primary Concern	National technology preferences (Art. 14, §1) and centralized authority powers may fragment the open architecture	Attention Needed

Dimension	Assessment	Main Risks
Internet Critical Properties	4 of 5 affected	Technological fragmentation, gatekeeping
Enablers	7 of 10 impacted	Restricted access, reduced diversity
Economic Impact	Moderate	Compliance costs, concentration
International Compatibility	Partial	Harmonization gaps

1. Introduction

This Internet Impact Assessment evaluates the Cybersecurity Legal Framework (PL 4752/2025), proposed by Senator Esperidião Amin, using the Internet Society's Internet Impact Assessment Toolkit (IIAT). The IIAT provides a structured methodology for identifying whether a policy, technology, or business practice may harm the Internet's fundamental architecture, threatening its global, open, secure, and trustworthy nature.

The Internet owes its strength and success to a foundation of critical properties that, when combined, represent the Internet Way of Networking (IWN). These include: (1) an accessible infrastructure with a common protocol; (2) a layered architecture implemented on interoperable building blocks; (3) decentralized management with distributed routing; (4) a common, global system of identifiers; and (5) a general-purpose and technology-neutral network. We therefore examine the effects of the proposal on the foundations of the IWN paradigm, on which the Internet relies to exist and thrive as an open, globally connected, secure, and trustworthy resource.

In addition to the IWN critical properties, the assessment also considers the enablers essential for the Internet to thrive as an open, globally connected, secure, and trustworthy resource, as defined by the Internet Society (ISOC): (I) Easy and unrestricted access; (II) Unrestricted use and deployment of Internet technologies; (III) Collaborative development, management, and governance; (IV) Unrestricted reachability; (V) Available capacity; (VI) Data confidentiality of information, devices, and applications; (VII) Integrity of information, applications, and services; (VIII) Reliability, resilience, and availability; (IX) Accountability; (X) Privacy.

This assessment does not constitute a legal opinion, nor does it endorse or oppose the legislation. Its purpose is to identify Internet-related risks and opportunities in order to inform the legislative process.

2. About PL 4752/2025

PL 4752/2025, known as the Cybersecurity Legal Framework, is a bill of the Brazilian Senate that seeks to establish a comprehensive legal framework for national cybersecurity governance. It creates the National Digital Security and Resilience Program and designates a competent national authority with normative, oversight, and audit powers.

In this regard, the bill emerges in a context of intense geopolitical reconfiguration of global digital infrastructure. Cybersecurity occupies a central position in debates on technological sovereignty, and different countries have responded to this challenge along radically different trajectories. The concept of digital sovereignty is inherently ambiguous and can be instrumentalized in two opposite ways: (i) sovereignty as capacity, which focuses on investment in education, proprietary infrastructure, and decision-making autonomy grounded in technical competence; and (ii) sovereignty as control, which seeks self-sufficiency through market restrictions and geographic preferences, often ignoring the structural interdependencies of the global technology supply chain.

Through the analysis that follows, we conclude that PL 4752/2025 contains elements of both trajectories, and it is precisely this ambiguity that grounds the present assessment. The aim, accordingly, is to identify, based on technical and comparative evidence, the mechanisms that may lead to technological fragmentation and to suggest alternatives that strengthen Brazil's resilience without compromising its participation in the global Internet.

2.1 Main Provisions

The provisions of the bill most relevant to this analysis include:

- Art. 4 – Designates a National Cybersecurity Authority with broad normative, oversight, and audit powers over public entities participating in the National Digital Security and Resilience Program.
- Art. 5 – Establishes minimum cybersecurity standards for the federal public administration, aligned with recognized national and international norms.
- Art. 12 – Creates mandatory incident notification obligations for federal entities and program participants.
- Arts. 13–15 – Imposes supply-chain risk governance requirements, including risk classification of technology suppliers.
- Art. 14, §1 – Establishes procurement preferences for national technology suppliers (products and services developed in Brazil).
- Art. 14, §2 – Grants the authority the power to restrict the use of discontinued or unsupported technology solutions.
- Art. 14, §3 – Creates a supplier risk-classification index managed by the national authority.

- Art. 18 – Establishes multi-stakeholder advisory councils and working groups.
- Arts. 19–21 – Creates capacity-building, education, and R&D programs to build national cybersecurity capability.
- Art. 25 – Establishes transparency and accountability requirements for the national authority.
- Art. 26 – Allocates 3% of the National Public Security Fund and 2% of fixed-odds betting revenues to cybersecurity.

2.2 Scope

The main scope of the bill is the Brazilian Federal Public Administration. Participation by private-sector entities and state/municipal governments is voluntary via accession to the National Program. Importantly, operators of critical infrastructure may be subject to sector-specific rules issued by the national authority.

4. Cross-cutting Impacts of the Proposal

Before analyzing each critical property and enabler individually (which will be done in the sections that follow), this section presents a cross-cutting analysis of PL 4752/2025, identifying dimensions that run across multiple aspects of the Internet's architecture. The aim is to provide the contextual, geopolitical, economic, and normative framing that grounds the specific assessment carried out below. A finding of impact does not imply that the legislation is flawed; rather, it may signal areas in which additional safeguards or clarifications may be warranted.

To shape this analysis and provide the interpretive framing, care was taken to analyze three cross-cutting dimensions that manifest across multiple aspects of PL 4752/2025: (i) the interplay between regulatory choices and the geopolitical conditions of digital infrastructure; (ii) the economics of public and private allocation of resources to digital security; and (iii) concrete normative gaps that affect security research, infrastructure software, and multi-stakeholder governance mechanisms.

In this context, the effectiveness of Coordinated Vulnerability Disclosure (CVD) policies and of provisions protecting researchers — a central topic within dimension (iii) — depends intrinsically on normative clarity, on the active participation of technical and civil-society communities, and on alignment with the socio-technical realities of the Global South.

Approaches centered solely on administrative obligations, or on a perspective focused exclusively on strictly commercial interests, tend to be insufficient to ensure systemic resilience, technological diversity, and agile incident response.[1]

Moreover, positive examples in the Global South, such as Chile's recent Cybersecurity Framework Law (Law No. 21.663), prioritize clear mechanisms for researcher protection, incentives for small-business participation, and transparent criteria for technical assessment. These elements strengthen both security and the quality of public spending without resorting to protectionism.

Conversely, diversity of arrangements, suppliers, and technologies is a central component of systemic robustness, and overly homogeneous environments tend to exhibit greater correlation of failures and cascading risks.[2]

In this context, it is worth noting that PL 4752/2025, by concentrating its obligations on the notification of incidents that have already occurred (Art. 12), intervenes at a late stage of the attack cycle — something the cybersecurity literature identifies as a known limitation of reactive models. Modern frameworks such as the NIST Cybersecurity Framework 2.0 and the Zero Trust architecture (NIST SP 800-207) reinforce that effective security requires continuous verification and real-time visibility, not merely static compliance. By not explicitly incorporating these paradigms, the bill misses an opportunity to strengthen the resilience of Brazil's digital infrastructure at the earliest stages of the attack chain.

Accordingly, PL 4752/2025 misses an opportunity by not explicitly incorporating these paradigms, confining itself to a logic of static compliance that may quickly become obsolete in the face of evolving threats. International experience with incidents such as SolarWinds (2020) and Log4Shell (2021) has demonstrated that the digital supply chain is a critical attack vector that transcends national borders, and that effective response depends on global cooperation, transparency in vulnerability disclosure, and the adoption of security protocols at the Internet's infrastructure layer, such as RPKI for routing security, DNSSEC for DNS integrity, and TLS 1.3 for confidentiality in transit.

This omission is particularly serious in the Internet context because vulnerabilities in widely used software — such as cryptographic libraries, DNS servers, and routing protocol implementations — affect the network's shared infrastructure, simultaneously compromising the security of multiple ecosystem participants.

---

[1] See : https://www.mdpi.com/2227-9709/10/3/71

[2] See https://www.sciencedirect.com/science/article/pii/S0925527323000221?via%3Dihub and https://thesai.org/Downloads/Volume16No6/Paper_72-Cybersecurity_and_the_NIST_Framework.pdf.

Indicators such as cost per effectively protected asset and a technological-diversity index make it possible to assess whether the regulatory arrangement is expanding resilience or merely generating more formal obligations.

Charting an effective regulatory path becomes even more critical once we take into account the geopolitical dimensions.

It is essential to distinguish between the two main political uses of the idea of "digital sovereignty": (i) one centered on capacity-building — through investment in professional training, R&D, and integration with local technical ecosystems — and (ii) another focused on control, which manifests through market restrictions and origin-based preferences.

Against this backdrop, the Brazilian model must also make a political choice about which type of digital sovereignty it will prioritize. The analysis of PL 4752/2025 (particularly the provisions on national procurement preferences and risk classification) suggests that the bill contains elements of both trajectories. The final balance between sovereignty-as-capacity and sovereignty-as-control is a central point of tension for preserving the Internet's critical properties, such as an Accessible Infrastructure with a Common Protocol (CP1), which is addressed below.

4.1 CP1 – An Accessible Infrastructure with a Common Protocol

⚠ Assessment: Low risk with negative potential

PL 4752/2025 does not directly address the Internet's protocols (TCP/IP, DNS, etc.) nor does it replace any existing standard. However, by defining minimum security conditions (Art. 5) based on 'recognized national and international norms,' the bill has an effect that may be applied indirectly to Internet protocols.

It is worth noting that the cumulative reference to national and international standards opens, in theory, the possibility that national standards could be prioritized to the detriment of international standardization — a path that could, in the extreme, lead to segmentation. That said, it is important to record that Brazil has no track record of adopting standards incompatible with international standardization, and there are no concrete indications that the bill has such an objective. The risk, therefore, is structural and prospective in nature, and does not stem from any manifest intent on the part of the legislator.

That said, the preference for domestic solutions and suppliers (Art. 14, §1) could generate an indirect risk if the development of local cybersecurity technologies is not necessarily aligned with the Internet's established protocols and international standards, potentially creating divergence from the common protocol stack that sustains global reachability.

The central question, however, is not whether to pursue technological sovereignty, but how that sovereignty is instrumentalized. There are two possible trajectories, and the bill, as currently drafted, does not make clear which one will be followed.

In this regard, sovereignty as capacity is the trajectory that strengthens the national ecosystem without threatening the shared global infrastructure. Under this logic, the State invests in training professionals, incentivizes domestic R&D in cybersecurity, fosters Brazilian firms capable of competing technically in the global market, and creates certifications that raise the quality threshold of national products. The result is that sovereignty is expressed as accumulated competence, not as closure.

Countries that have pursued this trajectory — such as Israel, Estonia, and more recently Chile — have built robust national cybersecurity ecosystems without fragmenting the common infrastructure. Brazil, indeed, already has instruments pointing in this direction in Arts. 19–21 of the bill itself, which create capacity-building and R&D programs. These provisions are precisely the kind of sovereignty-as-capacity that raises no concerns for CP1.

Sovereignty as control is the trajectory that creates preferences, restrictions, or exclusions based on geographic origin or non-technical criteria. Under this logic, the State not only invests in the national ecosystem but also insulates the public market from foreign suppliers, whether directly (through procurement preferences) or indirectly (through risk indices lacking transparent criteria).

The risk to CP1 arises when products deployed in public infrastructure do not correctly implement fundamental Internet protocols — such as IPv6, DNSSEC, TLS 1.3, or routing-security mechanisms such as RPKI. The adoption of technologies with incomplete or incompatible implementations may, over time, create operational inconsistencies in public infrastructure. In addition to affecting interoperability, the absence of these mechanisms also creates structural vulnerabilities, facilitating attacks such as BGP route hijacking, DNS poisoning, and communications interception.

To avoid this risk, the bill should require that any prioritized domestic solutions be fully compatible with the Internet protocol suite.

> *Recommendation: Explicitly require that all minimum cybersecurity standards adopted under Art. 5 be consistent with internationally recognized open Internet standards bodies (IETF, ICANN, ISO, ITU).*

4.2 CP2 – Open Architecture of Interoperable and Reusable Building Blocks

⚠ Assessment: Low risk with negative potential

The Internet's layered architecture makes it possible to build complex services out of modular blocks. Each layer (physical, link, network, transport, application) has well-defined, open protocols. For example, typical building blocks include the TCP transport protocol (for reliable delivery) and IEEE 802.11 (Wi-Fi) at the link layer. The bill does not break this architecture, since it does not define any proprietary block nor impose new mandatory modules. However, the open architecture depends on the ability of any actor to build solutions or services that interconnect with the Internet's building blocks without gatekeepers. Several provisions introduce gatekeeping dynamics:

- Art. 14, §1 (National Procurement Preferences): Prioritizing domestically developed products and services creates a preference for a subset of available technologies, which may limit the range of interoperable components depending on the strength of that prioritization. Although it does not prevent the contracting of foreign solutions, the preference creates a selection bias that may, in practice, reduce the range of interoperable components considered in public procurement, particularly if the criteria for applying the preference are not objectively defined.
- Art. 14, §2 (Restriction of Unsupported Solutions): The power to restrict discontinued software may be a sensible security measure; however, in the absence of clear criteria, it grants the authority discretion to exclude suppliers or families of technology.
- Art. 14, §3 (Supplier Risk-Classification Index): Although the substantive definition of risk-classification criteria should be left to regulation, the primary legislation should establish the procedure for its development and review, including mandatory multi-stakeholder consultation (via the Art. 18 councils), prior publication of the criteria, a review schedule, and appeal mechanisms for classified suppliers, so as to ensure that any restrictions apply equally to domestic and foreign suppliers on the basis of security merit, not origin.

It is important to distinguish that, among the cybersecurity solutions covered by the bill, those operating at the Internet's infrastructure layer — such as implementations of transport, routing, and name-resolution protocols — must remain compatible with the IETF's open standards to preserve the network's interoperability.

> *RRecommendation: Establish clear, publicly available, and objective criteria for decisions on supplier risk classification and technology restriction. Ensure that any restrictions apply equally to domestic and foreign suppliers on the basis of security merit, not origin.*

4.3 CP3 – Decentralized Management and a Common Distributed Routing System

⚠ Assessment: Low risk with negative potential

PL 4752/2025 does not directly address routing, autonomous systems, or root DNS operations. However, the audit powers conferred on the national authority (Art. 4) potentially reach any digital system, including routing systems. Based on the results of such audits, the authority may restrict the use of systems deemed insecure by members of the National Digital Security and Resilience Program (Art. 7). Thus, although routing infrastructure is not a direct object of the legislation, decisions by the authority could indirectly affect technological choices in matters of routing within the public sector.

The Internet's resilience derives significantly from its decentralized, multi-stakeholder governance. A national authority with the power to restrict technology solutions for a significant portion of Brazil's digital economy could, over time, consolidate control over critical Internet infrastructure decisions.

Moreover, sovereignty policies that rely on state "command and control" may frustrate critical properties such as decentralized management. In addition, if the authority's powers are subsequently extended — whether through subsidiary legislation or sector-specific rules (Art. 4) — to private operators of critical infrastructure and Internet service providers, the risk to decentralized management would be substantially greater.

On the other hand, there are opportunities: supply-chain risk management (Art. 13), if well implemented, can improve the resilience of public-sector routing. By requiring, for example, security certifications for network devices (firewalls, routers) used by the government, the bill strengthens the stability of the public network.

It is therefore recommended that the text of the law or its regulations be supplemented to establish that no mandatory routing modification shall be implemented without broad technical consultation.

> *Recommendation: Clearly limit the normative powers and scope of the authority in the primary legislation. Ensure that any extension to private-sector entities requires additional parliamentary approval. Require that decisions affecting Internet routing and addressing be made in coordination with NIC.br and CGI.br, and observe practices already established at the international level through ICANN, the IETF, and other relevant bodies.*

4.4 CP4 – Common Global Identifiers

✔ Assessment: Not Impacted

PL 4752/2025 contains no provisions that would affect DNS, IP addressing, routing identifiers, or other globally unique Internet naming and numbering resources, because it does not contemplate the creation of parallel naming systems, national DNS roots, or fragmentation of the global address space.

4.5 CP5 – A General-Purpose and Technology-Neutral Network

⚠ Assessment: Low risk with negative potential

The Internet was designed for multiple uses, without optimization for only one type of traffic. It was conceived from the outset as a general-purpose network, and technological neutrality allows it to serve purposes that were not anticipated at the time of design.

PL 4752 does not impose the use of a specific network architecture or protocol; therefore, neutrality of use remains preserved. However, the combination of national procurement preferences (Art. 14, §1) with the authority's power to restrict technology solutions (Art. 14, §2) introduces a selection bias that may, in practice, favor certain technology families or applications over others.

This preference creates a regulatory environment in which the choice of technology is no longer guided solely by functional and interoperability criteria, and instead incorporates variables of geographic origin and administrative compliance.

The indirect risk to CP5 lies in the fact that, over time, restricting the universe of solutions available to the public administration may limit the public sector's capacity to adopt emerging technologies that do not yet have a domestic version, creating a technological lag that undermines the general-purpose premise. In addition, if the risk-classification index (Art. 14, §3) operates with opaque criteria, suppliers of innovative technologies may be dissuaded from participating in the Brazilian public market, reducing the diversity of available solutions and, consequently, the network's capacity to serve unanticipated purposes.

As discussed in the cross-cutting analysis, the sovereignty-as-capacity trajectory (Arts. 19–21) is the one that best preserves CP5, by creating conditions for Brazilian solutions to be competitive.

By contrast, the sovereignty-as-control trajectory, resting on origin-based preferences and opaque risk-classification criteria (Art. 14, §3), may produce the opposite effect, creating a technological lag that undermines the network's general-purpose premise.

In addition, PL 4752/2025 must be interpreted in harmony with Law No. 12.965/2014 (Marco Civil da Internet), particularly in relation to Art. 9 (net neutrality), Art. 10 (traffic discrimination or degradation), and Art. 11 (application prioritization).

The National Cybersecurity Authority should not have the power to determine traffic prioritization or the blocking of specific protocols under a security justification, except in cases of proven active incidents and with judicial oversight. Moreover, with regard to the risk of Layer Fragmentation, if the risk-classification index (Art. 14, §3) results in restrictions based on specific protocols (e.g., blocking VPNs, Tor, or P2P protocols), this would constitute a violation of technological neutrality and could fragment the Internet's layered architecture.

> *Recommendation: Ensure that technology-selection criteria prioritize interoperability, conformance with open standards, and technical merit, so that the Internet's technological neutrality is preserved as a guiding principle of public cybersecurity procurement, and that sovereignty is achieved through capacity-building — conditioning any national preferences on the demonstration of conformance with open, interoperable Internet standards, and ensuring that the strengthening of the Brazilian ecosystem occurs through excellence rather than through restricted access to technologies. In addition, a provision should be included that: i) ensures no technological restriction violates the principle of net neutrality; ii) requires any blocking or filtering decisions to be temporary, proportionate, and subject to judicial oversight; iii) prohibits discrimination based on application type or protocol.*

5. Impact on the Enablers of an Open, Globally Connected, Secure, and Trustworthy Internet

Goal 1: Open Internet

5.1 E1 – Easy and Unrestricted Access

⚠ Assessment: Low risk with mixed potential

The bill does not impose direct access restrictions on end users or Internet service providers. However, the national procurement preferences for technology (Art. 14, §1) and the supplier risk-classification index (Art. 14, §3) could indirectly limit access to specific technologies and services for entities within the bill's scope.

If the risk-classification index effectively results in the exclusion of major international technology suppliers from Brazilian public-sector procurement, this would restrict public entities' access to a globally diverse technology ecosystem.

On the other hand, the bill promotes investment in cybersecurity (3% of the National Public Security Fund), which can finance better network infrastructure for under-served public agencies. This improves those agencies' Internet access (greater bandwidth, lower latency). To balance the impact, it is

recommended that the future Authority implement the risk index using strictly technical criteria (e.g., known vulnerabilities, history of failures) and that it allow competition from open-source or international solutions that demonstrate conformance.

It should be recalled that the Internet "does not obey borders": digital sovereignty efforts should expand internal capabilities without creating access gates.

> *Recommendation: The supplier risk index should be based on strictly technical criteria (vulnerabilities, history of failures), not on national origin, allowing competition from open and international solutions that demonstrate conformance.*

5.2 E2 – Unrestricted Use and Deployment of Internet Technologies

⚠ Assessment: Medium risk with negative potential

This is the enabler most directly at risk from PL 4752/2025. The combination of national procurement preferences (Art. 14, §1), the authority's power to restrict solutions (Art. 14, §2), and the supplier risk-classification index (Art. 14, §3) creates a framework in which technology deployment within the public sector is subject to centralized gatekeeping.

Historically, policies of this kind have been used not only for cybersecurity but also to advance industrial policy. In the Brazilian case, there is no explicit indication that different technical standards would be imposed, but the power to restrict outdated solutions gives the authority case-by-case discretion. This can cause technology suppliers to fear that updates may be blocked on risk grounds. Internationally, "technological sovereignty" policies tend to follow two paths: (i) they strengthen the domestic market (causing minimal harm to the Internet), or (ii) they increase state control (potentially fragmenting the network).

The Internet's architecture has thrived precisely because any participant can implement and innovate on top of its open protocols without gatekeepers; the introduction of centralized approval mechanisms, even with good intentions, can gradually erode this fundamental principle.

> *Recommendation: Define precise and exhaustive grounds for technology restriction in the primary legislation. Require multi-stakeholder public consultation for restrictions that affect multiple entities or classes of technology. Align the classification methodology with international frameworks to prevent arbitrary exclusions.*

5.3 E3 – Collaborative Development, Management, and Governance

✔ Assessment: Positive Impact

The provision of Art. 18 for multi-stakeholder advisory councils and working groups is an aspect that aligns with the Internet's collaborative governance principles. The inclusion of civil society, academia, the private sector, and government in cybersecurity standard-setting processes mirrors the multi-stakeholder model that sustains Internet governance at the global level.

Art. 3, V explicitly names inter-sectoral collaboration as a guiding principle of the National Program. Arts. 19–21, focused on education, training, and R&D, fostering a broader national ecosystem of cybersecurity expertise. The transparency requirements of Art. 25 further support responsible collaborative governance.

> *Recommendation: To maximize the positive impact of this enabler, advisory councils should have meaningful roles in decisions on standard-setting and technology restriction.*

Goal 2: Globally Connected Internet

5.4 E4 – Unrestricted Reachability

✔ Assessment: Not Impacted

PL 4752/2025 contains no provisions that would restrict the network's reachability, impose blocking mandates, or create routing restrictions.

Technologically, the Internet holds that an IP packet from server A should reach user B regardless of local policies. Connectivity thus grows as more participants connect. Reinforcing this point, Art. 2 of the bill highlights the continuity of digital communications as vital to technological sovereignty, which implies precisely maintaining international links.

The legislation does not seek content filtering, ISP obligations for traffic management, or cross-border data-flow restrictions. Unrestricted reachability at the network layer is not threatened by this bill.

5.5 E5 – Available Capacity

✔ Assessment: Positive Impact

The bill's significant funding provisions (Art. 26 allocating 3% of the National Public Security Fund and 2% of fixed-odds betting revenues to cybersecurity) will support infrastructure investments that contribute to network capacity and resilience.

By strengthening the cybersecurity posture of government systems, the legislation reduces the likelihood of large-scale cyber incidents that can degrade network capacity for all users.

The Art. 20 provisions for national cybersecurity R&D programs may also yield innovations that improve network performance and capacity management.

Goal 3: Secure Internet

5.6 E6 – Data Confidentiality of Information, Devices, and Applications

✔ Assessment: Positive Impact

The bill's general cybersecurity orientation — including minimum standards (Art. 5), a culture of cybersecurity (Art. 3, III), and training programs (Art. 19) — should promote the adoption of encryption and secure-communications practices across the public sector. Stronger cybersecurity postures in government reduce systemic risks that could compromise data confidentiality for citizens interacting with public services.

A further positive aspect is that the bill contains no provisions mandating backdoors, weakened encryption, or key escrow — measures that have undermined data confidentiality in other cybersecurity legislative frameworks.

Even so, it would be more forceful to explicitly state in the bill that strong encryption mechanisms must be permitted and indeed encouraged. If the national authority establishes cybersecurity standards (Art. 5), it makes sense for these to include encryption of data in transit (TLS 1.3, as a minimum) and at rest, as well as the adoption of security protocols at the infrastructure layer, such as DNSSEC, RPKI, and DMARC/SPF/DKIM for email security.

The absence of encryption restrictions in the text suggests that confidentiality can be maintained in line with international best practice, but making these requirements explicit in subsequent regulation by the Authority would strengthen the framework's security posture and signal a commitment to the security of the Internet's infrastructure layer.

Considering digital sovereignty in the sense of citizen protection, it is recommended to state explicitly that no rule will require the breaking of encryption or the excessive collection of personal data. Technologies such as VPNs, Tor, and end-to-end encryption should remain available for public and governmental use where needed, provided they are compatible with the law.

> *Recommendation: The bill should explicitly affirm that cybersecurity standards (Art. 5) include strong encryption in transit and at rest, and that no rule may require the breaking of encryption or the excessive collection of personal data.*

5.7 E7 – Integrity of Information, Applications, and Services

✔ Assessment: Positive Impact

Integrity means ensuring that data and systems are not improperly altered. PL 4752 emphasizes security controls that reinforce integrity. Art. 13 mandates supplier risk assessment and the mitigation of flaws across the chain, which implies regular audits and testing — practices that improve overall integrity.

Additionally, Art. 14, §2 allows the prohibition of outdated or insecure solutions, encouraging the use of patched software versions. For example, if a critical system has an SQL injection vulnerability, it would have to be replaced or updated so as not to appear on the prohibited list. When transparent, this kind of measure increases confidence that public services will be delivered free from tampering.

There are trade-offs, however. If the risk index is applied on non-technical grounds, there may be fewer high-integrity alternatives. For this reason, it is essential that the future Authority adopt international frameworks for integrity verification (e.g., cybersecurity maturity models) and permit third-party certifications so that a supplier can meet the criteria without discrimination.

Interoperability of logs and event records should also be encouraged, so that, for example, open log formats (JSON, standard syslog) are used, enabling independent auditing. By allowing any interested parties to review the integrity of public systems (as contemplated by the bill's transparency provisions), it is reinforced that public data and services will not be corrupted, maintaining integrity and strengthening principles that allow the Internet to remain global and secure.

Goal 4: Trustworthy Internet

5.8 E8 – Reliability, Resilience, and Availability

✔ Assessment: Positive Impact

Resilience is presented as a central objective of the bill. The requirement of Art. 11 for continuity and recovery policies directly addresses the resilience of government digital services. In addition, Art. 2, paragraphs I and XV, list as objectives strengthening cyber resilience and ensuring the continuity of digital communications even during a crisis.

In practice, this means that federal agencies must maintain multiple connection paths, redundant systems, and recovery plans. Technologies such as data replication, automatic failover, and software-defined networking (SDN) can be supported to improve the availability of government

systems. In addition, the incident-notification mechanism of Art. 12 creates a feedback loop that should improve collective resilience.

5.9 E9 – Accountability

✔ Assessment: Positive Impact

The transparency and accountability requirements of Art. 25 for the national authority are well aligned with this enabler. Accountability in cybersecurity means that actors know their obligations and face consequences for failures. The bill clearly states that public managers will be held accountable for implementing the rules and responding to incidents (Art. 2, XIII).

The bill establishes audit and oversight powers (Art. 4) that create accountability mechanisms for entities within its scope. The mandatory notification of incidents (Art. 12) also contributes to accountability by creating a record of security events and responses.

However, to reinforce the accountability chain, it is also recommended to include penalties for failing suppliers. For example, public technology contracts should contain Service Level Agreement (SLA) clauses providing for penalties if reported vulnerabilities are not remediated within the agreed timeframe. In addition, fiscal transparency (Art. 26, Chapter IV) reinforces that cybersecurity expenditures will be audited, which drives measurable outcomes. From the user's point of view, nothing changes directly; but for the infrastructure, it means that there will be documentation and accountability.

> *Recommendation: Include SLA clauses in public technology contracts with penalties for suppliers that fail to remediate reported vulnerabilities within the agreed timeframe, strengthening the accountability chain beyond public officials.*

5.10 E10 – Privacy

⚠ Assessment: Low risk with mixed potential

Privacy presents a mixed picture. On the positive side, Art. 3, XI explicitly lists the protection of privacy as a guiding principle of the National Program, and the bill is described as operating in harmony with Brazil's General Data Protection Law (LGPD).

It is true that the bill does not directly regulate personal data; still, any increase in governmental oversight of networks may raise privacy concerns. Technically, it is recommended to address privacy by design: for example, requiring federal systems to use encryption for sensitive data and to collect only what is necessary for security. A concrete measure would be to require all government networks to use

VPNs or end-to-end encryption for internal communications, following global standards. In addition, as a safeguard, audit bodies (internal and CGU) should act to ensure that any surveillance or data-collection activity under the bill respects the LGPD.

Therefore, the incident-notification obligations (Art. 12), if they involve sharing personal data of affected individuals with the national authority, must have their scope carefully defined to comply with the LGPD's proportionality principles. The authority's audit and oversight powers (Art. 4) over government systems create broad access to sensitive data and require robust legal safeguards and oversight mechanisms.

> *Recommendation: Require that incident reports (Art. 12) use anonymized or pseudonymized data by default, and that audit powers (Art. 4) be exercised with explicit proportionality safeguards aligned with the LGPD.*

6. Impact Table

The tables below provide a consolidated view of the assessed impact of PL 4752/2025 on the Critical Properties of the Internet Way of Networking and on the OGST Enablers.

6.1 Critical Properties

Ref.	Critical Property	Assessment	Detail
CP1	Accessible Infrastructure with a Common Protocol	CONCERN	Limited
CP2	Open Architecture of Interoperable and Reusable Building Blocks	CONCERN	Moderate
CP3	Decentralized Management and Single Distributed Routing System	CONCERN	Limited
CP4	Common Global Identifiers	NO IMPACT	–
CP5	General-Purpose and Technology-Neutral Network	CONCERN	Moderate

6.2 HOGST Enablers

Ref.	Goal	Enabler	Assessment	Dir.
E1	Open	Easy and Unrestricted Access	MIXED	~

Ref.	Goal	Enabler	Assessment	Dir.
E2	Open	Unrestricted Use and Deployment of Internet Technologies	CONCERN	–
E3	Open	Collaborative Development, Management, and Governance	POSITIVE	+
E4	Global	Unrestricted Reachability	NO IMPACT	–
E5	Global	Available Capacity	POSITIVE	+
E6	Secure	Data Confidentiality of Information, Devices, and Applications	POSITIVE	+
E7	Secure	Integrity of Information, Applications, and Services	POSITIVE	+
E8	Trustworthy	Reliability, Resilience, and Availability	POSITIVE	+
E9	Trustworthy	Accountability	POSITIVE	+
E10	Trustworthy	Privacy	MIXED	~

7. Recommendations

7.1 Positive Aspects

PL 4752/2025 contains several provisions that represent positive contributions to the resilience and trustworthiness of the Internet in Brazil:

- Dedicated funding for cybersecurity (Art. 26), whose adequacy to the volume of incidents within the scope of the law will need to be assessed on the basis of data allowing the actual demand to be sized.
- Mandatory notification of incidents (Art. 12) creates institutional accountability and enables collective learning.
- Supply-chain risk governance (Arts. 13–15) addresses a critical contemporary threat vector.
- Multi-stakeholder advisory councils (Art. 18) and collaboration as a guiding principle (Art. 3, V) align with Internet governance best practices.

- Transparency and accountability requirements (Art. 25) support democratic oversight.
- Alignment with the LGPD and privacy as a guiding principle (Art. 3, XI).
- The bill avoids the most harmful cybersecurity-legislation patterns: there are no encryption backdoor requirements, content-filtering mandates, routing restrictions, or data-localization obligations, thereby preserving the fundamental properties of the Internet Way of Networking.

7.2 Areas of Concern

The following provisions of PL 4752/2025 create risks for the Internet's open and interoperable architecture and should be addressed during the legislative process:

- National Technology Procurement Preferences (Art. 14, §1): Economic protectionism in technology procurement, if extended to security-relevant software and infrastructure, risks creating incompatible technology stacks and reducing the diversity of interoperable components available to Brazilian public entities.
- Centralized Restriction Powers (Art. 4 and Art. 14, §2): The national authority's power to restrict technology solutions, without clearly defined criteria, due process, or proportionality requirements in the primary legislation, creates a gatekeeping mechanism that could be misused.
- Supplier Risk-Classification Index (Art. 14, §3): Without transparent, internationally aligned criteria and meaningful appeal mechanisms, this index could function as a de facto blocklist, reducing technological diversity and creating barriers for international suppliers.
- Supplier Risk-Classification Index (Art. 14, §3): Without transparent, internationally aligned criteria and meaningful appeal mechanisms, this index could function as a de facto blocklist, reducing technological diversity and creating barriers for international suppliers.
- Absence of Provisions on Coordinated Vulnerability Disclosure: The bill does not provide mechanisms to protect good-faith security researchers nor deadlines for vendor remediation. This gap may discourage independent security research, prolong exposure to critical vulnerabilities in shared Internet infrastructure, and weaken the cyber defense chain at its earliest stages.

7.3 Legislative Recommendations

Based on this analysis, the following specific legislative amendments and implementation measures are recommended to strengthen the alignment of PL 4752/2025 with the principles of the Internet Way of Networking:

#	Provision	Recommendation
R1	Art. 14, §1 (Procurement Preferences)	Replace preferences based exclusively on national origin with recognized security-certification requirements — whether international (Common Criteria, ISO 27001, FIPS 140-3) or national — provided they are based on objective technical criteria and applied on a non-discriminatory basis to all suppliers. In addition, consider including requirements for the handling of critical data within national territory as a complementary security criterion, aligned with the LGPD and with international practices for the protection of sensitive data.
R2	Art. 14, §2 (Restriction Powers)	Define in the primary legislation the exhaustive list of grounds for technology restrictions. Require prior multi-stakeholder consultation (Art. 18 councils) and a proportionality assessment before imposing restrictions. Create an expedited appeal process.
R3	Art. 14, §3 (Supplier Risk Index)	Require the classification methodology to be developed through the multi-stakeholder process of Art. 18, published in advance, and aligned with international risk frameworks (NIST SP 800-161, ENISA). Require annual public reports and independent audits of classification decisions.
R4	Art. 4 (Authority's Scope)	Clarify in the primary legislation that the authority's normative powers apply exclusively to federal public-administration entities enrolled in the Program. Any extension to private-sector entities must require separate parliamentary authorization.
R5	Art. 5 (Minimum Standards)	Explicitly require that all minimum cybersecurity standards adopted by the authority be compatible with Internet standards from the IETF, ISO, and ITU-T. The standards must not require proprietary protocols or exclude open-source solutions.
R6	Arts. 12 and 4 (Notification and Audit)	Specify that incident reports must use anonymized or pseudonymized technical data by default. Establish judicial-oversight requirements for the authority's access to personally identifiable information. Require Data Protection Impact Assessments (DPIAs) for the authority's core data-processing functions.
R7	Art. 18 (Multi-stakeholder Councils)	Elevate advisory councils to the status of mandatory consultation for all normative decisions affecting Internet architecture, including technology restrictions, supply-chain rules, and minimum standards. Require council recommendations to be published alongside the authority's decisions.
R8	New provision (Coordinated Vulnerability Disclosure and	Include provisions on Coordinated Vulnerability Disclosure with safe harbors for good-faith researchers and deadlines for vendor remediation. Incorporate into the minimum standards (Art. 5) the requirement to adopt security protocols at the

#	Provision	Recommendation
	Infrastructure Protocols)	Internet's infrastructure layer (RPKI, DNSSEC, TLS 1.3, IPv6) as mandatory requirements for entities participating in the Program.
R9	Art. 3 (Definitions)	Add a definition of strong encryption in the following terms: "cryptographic algorithms, protocols, and implementations that meet, cumulatively, the following requirements: a) offer a level of security consistent with the state of the art recognized by international standards bodies (IETF, NIST, ISO/IEC) and by the technical community, in accordance with regulations issued by the competent authority; b) do not contain intentional vulnerabilities, exceptional-access mechanisms (backdoors), or features allowing third parties, including the developer itself, to bypass the cryptographic protection mechanisms; c) allow, where applicable, independent conformance verification through technical audit, peer review, and/or publication of the source code."
R10	Art. 3 (Guidelines)	Add a prohibition of cryptographic backdoors: "XVI – protection of cryptographic integrity: no rule, regulation, or administrative decision may: a) require the inclusion of vulnerabilities, exceptional-access mechanisms, or interception features in systems, applications, or protocols using encryption; b) require the custody, deposit, or sharing of private cryptographic keys with a third party; c) determine the weakening, replacement, or non-adoption of cryptographic algorithms, protocols, or implementations recognized by the international technical community, or influence the setting of cryptographic standards other than to promote a higher level of security; d) prevent or restrict the use of end-to-end encryption by users, public entities, or service providers."
R11	Art. 5 (Minimum Standards)	Add specific cryptographic requirements: "§ 2. The minimum cybersecurity standards referred to in the caput shall include requirements for cryptographic protection, observing the following principles: I – for data in transit: use of secure-communications protocols that guarantee confidentiality, authenticity, and forward secrecy, in accordance with the prevailing open standards recognized by international standards bodies; II – for data at rest: use of internationally recognized symmetric-encryption algorithms, with secure management of the cryptographic-key life cycle, including generation, storage, rotation, and destruction; III – for critical infrastructure: adoption of security mechanisms at the Internet's infrastructure layers, including route-origin authentication, integrity of domain-name resolution, and support for the most recent version of the Internet Protocol, in accordance with standards developed in the competent technical forums. § 3. The competent authority shall publish and keep up-to-date, within a period not exceeding 12 months from the entry into force of this Law and reviewed at least every 24 months, a reference list of the algorithms, protocols, and technical

#	Provision	Recommendation
		parameters that meet the requirements of § 2, taking into account the recommendations of Internet standards bodies (IETF), NIST, ISO/IEC, and other recognized bodies."
R12	New provision (Coordinated Vulnerability Disclosure)	Add Section XI to Chapter III: "Art. 25-A. The competent authority shall establish a coordinated vulnerability disclosure program, observing the following principles: I – legal protection of security researchers who identify and report vulnerabilities in good faith, in accordance with the coordinated-disclosure policies published by the authority; II – establishment of deadlines proportionate to the severity of the vulnerability for vendors and developers to implement fixes, in accordance with a criticality classification defined in regulation; III – publication of clear, accessible policies regarding scope, permitted methodology, reporting channels, and good-faith criteria; IV – prohibition of administrative, civil, or criminal sanctions against researchers acting in strict compliance with the coordinated-disclosure policies, save in cases of intent or manifest deviation from the authorized scope; V – encouragement of Brazilian entities' participation in international incident-response and vulnerability-disclosure communities. Sole paragraph. The deadlines referred to in item II shall be set by regulation, after consultation with the advisory councils referred to in Art. 18, and reviewed periodically in light of international best practice."
R13	Art. 14, §1 (National Preferences)	Amend the wording to: "§ 1. The prioritization of suppliers and technologies under the Program shall observe, cumulatively, objective and non-discriminatory criteria based on: I – demonstrable conformance with technical security standards recognized by international standards bodies; II – traceability and transparency of the supply chain, including the identification of critical components and their dependencies; III – the ability to carry out independent auditing and integrity verification of software and hardware components; IV – jurisdictional risk assessment based on technical and objective criteria, taking into account the legal framework applicable to the supplier in matters of governmental access to data and systems. § 2. The criteria set out in § 1 apply equally to domestic and foreign suppliers, and discrimination based solely on the geographic origin of the supplier or technology is prohibited. § 3. The methodology for assessing the criteria shall be developed with the participation of the multi-stakeholder councils referred to in Art. 18, published in advance, and reviewed at least every 24 months. V – availability of source code for independent auditing, with a preference, under equal technical and security conditions, for solutions distributed under free or open-source software licenses recognized by the Open Source Initiative (OSI). Sole paragraph. The preference for open-source solutions referred to in item V does not exclude

#	Provision	Recommendation
		proprietary solutions that demonstrate conformance with the other criteria and that allow independent auditing through equivalent mechanisms."

8. Conclusion

PL 4752/2025 reflects a legitimate and necessary effort to strengthen Brazil's national cybersecurity posture. The bill's central objectives — improving the resilience of government digital systems, establishing a coordinated incident-response capability, and building national cybersecurity expertise — are aligned both with international best practice and with the Internet Society's vision of a secure and trustworthy Internet.

However, the bill's impact on the Internet is not uniformly positive. The national technology procurement preferences (Art. 14, §1) and the centralized technology-restriction powers (Art. 4, Art. 14, §§2–3) introduce risks to the open and interoperable architecture that makes the Internet globally valuable. These provisions, if implemented without adequate safeguards, could fragment Brazil's technology ecosystem, reduce access to the global diversity of interoperable building blocks, and set a precedent for technological gatekeeping justified on cybersecurity grounds.

The identified risks are not inherent to the bill's objectives; they arise from specific implementation choices that can be addressed through targeted legislative amendments. The recommendations in Section 7 provide a concrete roadmap for strengthening the bill's alignment with the principles of the Internet Way of Networking without compromising its cybersecurity objectives.

The Internet Society encourages legislators, the designated national authority, and civil-society stakeholders to engage with this analysis as part of the legislative process. A cybersecurity framework designed from the outset with respect for the Internet's architectural principles will be more effective, more durable, and more compatible with Brazil's role as a leading actor in global Internet governance.

Annex I – Glossary of Technical Terms

Term	Definition used
End-to-End Encryption (E2EE)	A communication model in which data are encrypted on the originating device and decrypted only on the destination device, with no intermediaries (including service providers) having access to the content in plaintext.
Gatekeeping	Centralized control exercised by an entity (public or private) over access to technologies, markets, or infrastructures, which may limit the diversity of available solutions and competition.
Technological Neutrality	The principle that the network does not discriminate on the basis of the technology, protocol, or application used, allowing the Internet to serve purposes not anticipated at the time of its design.
Coordinated Vulnerability Disclosure (CVD)	A structured process of responsible reporting of security flaws, in which the researcher notifies the vendor before public disclosure, allowing the vulnerability to be fixed within agreed timeframes.
DNSSEC (Domain Name System Security Extensions)	A set of security extensions to the DNS protocol that authenticate responses to domain-name queries by means of digital signatures, preventing attacks such as DNS cache poisoning.
RPKI (Resource Public Key Infrastructure)	A public-key infrastructure that enables the cryptographic validation of the origin of BGP (Border Gateway Protocol) route announcements, preventing route hijacking and malicious traffic redirection on the Internet.
Perfect Forward Secrecy (PFS)	A property of cryptographic protocols that ensures derived session keys cannot be retroactively compromised, even if the server's long-term private key is later exposed.

BGP (Border Gateway Protocol)	The inter-domain routing protocol that enables the exchange of reachability information between autonomous systems on the Internet. Vulnerabilities in BGP can enable route hijacking and traffic redirection.
CSIRT (Computer Security Incident Response Team)	A specialized team that receives, analyzes, and responds to cybersecurity incidents, coordinating mitigation and recovery actions.
Cyber Kill Chain	A model developed by Lockheed Martin that describes the seven sequential stages of a cyber attack: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and actions on objectives.
TLS (Transport Layer Security)	A cryptographic protocol that ensures the confidentiality and integrity of Internet communications. Version 1.3 (TLS 1.3), published in 2018, is the most recent and secure version and is recommended as the minimum standard.
Zero Trust	A cybersecurity model (NIST SP 800-207) that eliminates implicit trust in any component of the network, requiring continuous verification of identity, device, and context for every access to resources.

Annex II – International Compatibility Analysis

Framework	Dimension	Convergence	Observation
NIS2 (EU)	Mandatory incident notification	CONVERGENT	Art. 12 of the bill. Without staggered deadlines equivalent to NIS2's (24h/72h).
NIS2 (EU)	Supply-chain governance	CONVERGENT	Arts. 13–15 of the bill address supply-chain risks.
NIS2 (EU)	Designation of national authority	CONVERGENT	Art. 4 designates an authority with normative, oversight, and audit powers.
NIS2 (EU)	Differentiated sectoral requirements	GAP	NIS2 differentiates between essential and important entities. The bill does not adopt an equivalent sectoral classification.
NIS2 (EU)	Cross-border cooperation	GAP	NIS2 creates the EU-CyCLONe. The bill mentions international cooperation (Art. 3, X), but without operational mechanisms.
DORA (EU)	Digital operational resilience	PARTIAL	Arts. 5 and 13–15 address standards and risks, but without DORA's specificity for the financial sector.
DORA (EU)	Resilience testing	GAP	No provision for mandatory penetration testing. Art. 5 may address this via regulation.
DORA (EU)	Oversight of critical third-party ICT providers	GAP	DORA establishes direct oversight of critical providers. The bill has no equivalent mechanism.
GDPR (EU)	Security of processing (Art. 32)	PARTIAL	The bill references the LGPD (Art. 3, XI), but does not articulate technical requirements equivalent to Art. 32.
GDPR (EU)	DPIA and Privacy by Design (Arts. 35, 25)	GAP	No provision for impact assessments or data protection by design for the authority.

Framework	Dimension	Convergence	Observation
GDPR (EU)	Coordination with the data-protection authority	GAP	No formal mechanisms for coordination between the cybersecurity authority and the ANPD.
Cooperation	International CSIRT networks	GAP	No mandatory participation in global communities (FIRST, regional CSIRTs).
Cooperation	Interoperability with alert systems	GAP	No interoperability requirements with global threat-sharing platforms.
Cooperation	Joint international exercises	GAP	Art. 3, X mentions cooperation, but without institutionalized participation in exercises.