**ORGANIZACIÓN DE LOS ESTADOS AMERICANOS**
**ORGANIZATION OF AMERICAN STATES**

**Comisión Interamericana de Telecomunicaciones**
**Inter-American Telecommunication Commission**

**45 MEETING OF PERMANENT CONSULTATIVE COMMITTEE I: TELECOMMUNICATIONS/ INFORMATION AND COMMUNICATION TECHNOLOGIES**
**August 19 to 23, 2024**
**João Pessoa, Brazil**

**OEA/Ser.L/XVII.4.1.45**
**CCP.I-TIC/doc. 5644/24 rev. 1**
**14 August 2024**
**Original: English**

# IMPROVING CYBERSECURITY IN DIGITAL PUBLIC INFRASTRUCTURE AND ARTIFICIAL INTELLIGENCE

**(Item on the Agenda: 4.2.3)**

**(Document submitted by the Delegation of Brazil)**

**Impact on the sector:**

This document aims to inform about Brazilian perspectives concerning the connections between cybersecurity and the agendas of digital public infrastructures and artificial intelligence, particularly focusing on capacity-building and awareness, which leads to the needs to modify und update Resolution 50 and its implementation.

**Executive Summary:**

This contribution aims to present a perspective on the topics of privacy, data protection, and cybersecurity in the Brazilian context, linking them with the international debate occurring under Brazil's presidency of the G20 and the global discussions around the Global Digital Compact. The contribution also highlights the role of cybersecurity, data governance, and data protection in two main areas: Digital Public Infrastructure and Artificial Intelligence.

## 1. Context

In 2024, under Brazil's G20 presidency, there is a strong emphasis on advancing the digital agenda, particularly focusing on the development of digital public infrastructures (DPIs) and the use of artificial intelligence (AI). Brazil aims to leverage these technologies to drive economic growth, enhance public services, and bridge the digital divide. The country is pushing for greater investment in digital public infrastructures, such as data centers and research and development, besides trying to ensure widespread access and digital literacy with investments in education. Additionally, Brazil is advocating for an approach regarding AI as a tool to promote sustainable development and to overcome inequalities instead of deepening gaps.

Therefore, data governance and cybersecurity are essential pillars for the successful implementation of these digital policies. Effective data governance ensures that data is managed in a manner that is transparent, secure, and respects user privacy. This is particularly important as the digital transformation increases the volume and sensitivity of data being collected and processed. Cybersecurity is equally critical, as it protects digital infrastructures from threats and vulnerabilities that could undermine trust and stability. This is the reality not just for Brazil, but for several countries that are trying to keep pace with digital transformation processes. That is why standardization and cooperation on cybersecurity, in an inclusive manner, can create a secure and resilient digital environment that can support innovation, protect citizens, and foster international collaboration in the digital realm.

One of the major challenges that states face today in the development of DPIs is data security and the trust that the population needs to place in these services. Therefore, awareness programs and the promotion of these services should be prioritized in their implementation.

Another issue that has been prioritized by the Brazilian presidency at the G20 is meaningful connectivity and the need to improve access to digital public services. Research from CETIC.br[1] shows that disparities between women and men are perpetuated in digital access, creating challenges for governments in implementing digital services and information and preventing vulnerable groups, including women, from fully accessing services and information through digital means.

In the last week of July 2024, the Brazilian National Committee on Science and Technology also launched a National AI Plan[2], which outlines a series of immediate impact actions in various areas such as public service management and education. A key proposal is the creation of a robust ecosystem of public data in a sovereign cloud, to ensure national technological autonomy, the integrity and security of information, and the privacy of citizens. Accordingly, there is a set of privacy and security actions within federal agencies, particularly to guarantee citizens' privacy in the provision of public services.

## 2. Right to Privacy in the Digital Age

Brazil has a history of spearheading privacy and data protection actions in Latin America. In this context, the 2013 and 2014 UN General Assemblies adopted two resolutions co-sponsored by Brazil and

[1] CETIC.BR. Year XVI - N. 2 - Technologies for public services: https://cetic.br/pt/publicacao/year-xvi-n-2-technologies-for-public-services/.

[2] G20 Brasil. Brasil launches a USD 4 billion plan for AI and prepares global action: https://www.g20.org/en/news/brasil-launches-a-usd-4-billion-plan-for-ai-and-prepares-global-action.

Germany (69/166 and 68/167)[3] [4]. Both resolutions address issues related to privacy in the digital age and stress that mass surveillance can threaten democratic freedoms and privacy rights[5].

Alongside the international arena, Brazil has had significant national milestones related to the protection of privacy and data, now recognized as constitutional rights. Brazil approved the Marco Civil da Internet (Brazil's Internet Bill of Rights) in 2014. This seminal document establishes rights and obligations for all internet users in the country, with data protection and privacy as two of its guiding principles.

Although data protection in Brazil has been addressed by other legal instruments, such as the constitutional remedy *Habeas Data* and the broader consumer protection ecosystem, Brazil further advanced in 2018 with the approval of the General Data Protection Law (LGPD). This law created a legal framework for data processing in the country, establishing rights and obligations for all parties involved.

Four years after the LGPD was approved, Constitutional Amendment 115 was enacted, which altered the Brazilian Constitution to include data protection as an autonomous and fundamental right. This change in the status of data protection in Brazil, which led to its constitutional recognition, reinforces the need to ensure both privacy and protection of Brazilian citizens' data. The recognition of data protection and privacy as constitutional rights should serve as a foundation for a robust data governance culture, which will help guarantee the protection of these rights.

Although privacy, data protection, and information security have different meanings, they are complementary subjects. In this sense, the Brazilian Federal Government approved the National Framework on Information Security (PNSI) in 2018, as part of the Brazilian Strategy on Cybersecurity (E-Ciber). This framework addresses cybersecurity, cyber defense, critical infrastructure security – such as the telecommunication sector –, protection against data leaks, and also emphasizes education and public awareness on cybersecurity issues as one of its principles. Both the E-Ciber and the PNSI can be used as important tools for raising awareness and building citizens' capacity to handle cybersecurity issues.

## 3. New agendas: AI and DPI

As previously mentioned, there are two areas highlighted in the digital economy agenda , which demand attention in regard to cyber security measures: Artificial Intelligence (AI) and Digital Public Infrastructure (DPI). Therefore, harmonizing different initiatives about these areas is of crucial importance. In this sense, initiatives on AI, like the new Brazilian National AI Plan, should also relate to other international initiatives -such as AI For Good, created by the ITU.

The current Brazilian legislative debate addresses artificial intelligence systems as machine-based systems that, with different degrees of autonomy and for explicit or implicit purposes, infer, from a set of data or information it receives, how to generate results, in particular, prediction, content, recommendation or decision that can influence the virtual, physical or real environment. Digital public infrastructures are defined by the Executive Branch as structuring solutions with transversal application, which adopt network technology standards built for the public interest, follow the principles of universality and interoperability, allow use by various entities in the public and private sectors and can integrate services in physical and digital channels (Decree 12,069/2024).

The above-mentioned Brazilian AI plan brings forward a strong focus on cybersecurity, pushing for investments in AI systems development to improve detection and response for cybersecurity incidents in government. This poses a challenge, particularly concerning capacity development within the

[3] German Brazilian resolution on internet privacy adopted: https://www.auswaertiges-amt.de/en/aussenpolitik/internationale-organisationen/vereintenationen/131127-resolution-privatsphaere-im-internet/258450.

[4] SANTORO, Mauricio; BORGES, Bruno. Brazilian Foreign Policy Towards Internet Governance: https://www.scielo.br/j/rbpi/a/TCv9k9dPmfrS8TH5G67ctbn/#

[5] Ibid.

government. In this sense, the implementation of the plan could include the interaction with these initiatives that have been leading the efforts on AI internationally for years.

ITU's work on AI, based mainly on Plenipotentiary Conference RES 214 (*Artificial intelligence technologies and telecommunications/ information and communication technologies*), focus on fostering robust telecommunication/ICT ecosystems in order to support AI, and also towards applying AI to make telecommunications/ICTs more efficient. Robustness relies on security.

This means that besides the Union initiatives like AI for Good, related to the benefits of AI for sustainable development, and the ITU AI repository, and specially considering ITU T cycle there is still room for attention to cybersecurity aspects, such as in the implementation of ITU T RES 50 Cybersecurity.

At the CITEL level, the implementation of COM/CITEL DEC. 117 (XLI-23) *Invitation to Study the Topic of Artificial Intelligence in the Work of PCC.I* might also consider cybersecurity aspects for the same reason of robustness.

Also, in the international plan, the UN has been leading the Universal Safeguards for DPI initiative. As shown in the initiative's first interim report[6], there is a strong concern of the international community with cybersecurity regarding the adoption of these technologies, particularly by governments. The initiative highlights that safety in DPI should be built through data governance and cybersecurity measures that enhance user's trust in these systems, something that surpasses the technology implementation, involving the level of experience of the diverse stakeholders in the DPI ecosystem with the technologies.

The report also points out that building trust requires transparency measures such as the periodical publication of impact assessment reports, providing indicators on cybersecurity and how it could be enhanced. The development of these reports is something that is also determined in the Brazilian National AI Plan and the proposed legislation on AI.

In this sense, both initiatives present a focus on cybersecurity from the perspective of capacity development, highlighting the need to have strong organizational understandings of the systems deployed. States also need to invest not only in the development of DPIs but also in user training and awareness. A notable example is PIX, an instant payment system that is one of the most successful DPIs in Brazil and has greatly promoted financial inclusion. However, it is expected to lose about USD 635.6 million to scams by 2027, according to the Scamscope Fraud Report developed by ACI Worldwide in partnership with Global Data[7]. Beyond information security knowledge, many scams are carried out through social engineering, which calls for public policies in this area as well.

In Brazil, another one of the most prominent systems framed as a DPI, the Electronic Information System (SEI), was recently the target of a cybersecurity attack that rendered the system offline for several days, impacting dozens of ministries and government agencies. SEI plays a crucial role in the digital processing of administrative procedures, enabling the creation, editing, processing, signing, and electronic filing of documents, which significantly reduces the reliance on paper and expedites information exchange.

Originally developed in 2009 by employees of the Federal Regional Court of the 4th Region (TRF4), which serves the southern region of the country, SEI has since evolved into its fourth version and is now employed by over 300 government agencies nationwide, including more than 120 within the federal government. The management of SEI is decentralized, meaning that each agency is responsible

[6] United Nations. Leveraging DPI for Safe and Inclusive Societies: https://1945836565-files.gitbook.io/~/files/v0/b/gitbook-xprod.appspot.com/o/spaces%2FcO6RXQuE2L2kjyKRy5qr%2Fuploads%2FJZlr3rRGWijWRI3zxHKL%2FLeveraging%20DPI%20for%20Safe%20and%20Inclusive%20Societies.pdf?alt=media&token=7e1ee3a2-89ab-4316-b7fc-eef01b353f90

[7] ACI Worldwide. ACI Worldwide Scamscope Report Finds APP Scam Losses Expected To Hit $6.8 Billion by 2027: https://investor.aciworldwide.com/news-releases/news-release-details/aci-worldwide-scamscope-report-finds-app-scam-losses-expected

for its own access and database management. As a result, an attack that disrupts SEI within the Ministry of Management does not necessarily affect the system's operation in other agencies. The SEI case underscores the importance of system architecture and DPI configurations in mitigating the impact of cybersecurity incidents.

Following this argument, and also shifting to international cooperation in the digital agenda, the current debate and negotiations related to the UN-led initiative of the Global Digital Compact (GDC) also presents approaches on cybersecurity that focuses on capacity development and skilling in non-military domains.

## 4. Conclusion

Facing new challenges and a broader scenario that encompasses axis related to DPI and AI, including data protection, ITU T RES 50 Cybersecurity and its implementation might be updated to highlight and strengthen security for new and emerging telecommunication/ICT services and technologies to be supported by the global infrastructure, such as AI driven ones.