CEST Centro de Estudos Sociedade e Tecnologia
USP Universidade de São Paulo
Bulletin – Volume 9 Number 03, May 2024

Navigating Chaos: the (In)Governance of Data Protection law in the face of AI

Thiago Felipe S. Avanci, Ph.D.

Em um In an increasingly interconnected and technologically advanced world, the protection of personal data emerges as an unprecedented challenge. In this context, Brazil's General Data Protection Law (LGPD) stands as a significant milestone in regulating the collection, use, and sharing of personal information. However, as technology advances rapidly, particularly in the field of artificial intelligence (AI), the current legislation faces a tough test: staying relevant in an environment characterized by constant innovation and uncertainty. Technological evolutions have proven to be true chaotic fractals in the short term, leading to an exasperated attempt at governance, especially when it comes to data security and its interaction with AI.

Data protection is not just a technical or legal issue but also a deeply social and ethical one.

The dynamics of AI, in particular, stand out as a vector of legal and ethical complexity. Firstly, there is still no ready national governance framework for AI in Brazil. Nonetheless, while the LGPD seeks to establish clear and effective norms for data protection, the autonomous and often unpredictable nature of AI systems presents a formidable challenge. These systems are designed to learn and adapt through data and experiences, theoretically evolving beyond their initial settings. This capability of self-learning and independent evolution calls into question the effectiveness of regulations that assume predictability and complete control over data. The central issue that arises is the suitability of the LGPD in the context of technologies that not only process data but also generate new data and behaviors without explicit human intervention. The current law focuses on principles such as transparency, consent, and data security, essential to ensuring that individuals maintain control over their personal information. However, with AI, these principles are tested by systems that can create, infer, and even act on data in ways not fully anticipated by their developers.

Moreover, the interoperability and integration of AI systems across various platforms and services exacerbate the transparency issue. The processing of data on a large scale and within complex information networks makes tracking the flow of personal data extremely challenging, undermining the principles of informed consent that underpin the LGPD. In this environment, the premise that an individual can effectively understand and control how their data is used becomes less viable. This scenario suggests that, in addition to continuously updating and adapting legislation, it is also necessary to reexamine and possibly redefine fundamental concepts of privacy and data protection. One possible approach would be the incorporation of AI ethics principles directly into data protection legislation. This would include specific guidelines on the development, use, and governance using AI systems, ensuring these technologies promote human welfare and operate according to fundamental ethical values.

To contextualize the issue, consider the current challenge of Generative AI (GenAI). In summary, this AI model, from user input, generates output created mathematically/statistically through a process of reading data from context windows for tokenization. For instance, OpenAI's GPT-3 chat used 8,192 tokens while version 3.5 used 16,385, version 4 used 32,768 tokens, and the latest version, GPT-4o, uses 128,000, an evolution that occurred from September 2021 to May 2024.

In this latest version, for each key point of user input, it analyzes 128k words, which is equivalent to 300 pages of text. Thus, for each generated point, this version of GenAI analyzes 300 pages of text to generate a response. With this, the astute reader should have grasped the challenge of GenAI vs. the LGPD...

Perhaps with the creation of more flexible and dynamic governance mechanisms, capable of responding quickly to new technological realities, there would be a better perspective for adjusting to the rapidly broken technological boundaries. This could involve the formation of specialized committees or agencies that work together with technology developers, ethics experts, and the general public to monitor the impact of AI on privacy and data security and propose regulatory adjustments as needed. However, more adaptive governance does not imply an absence of oversight since the enforcement of regulations also needs to be strengthened. This would involve not only imposing more severe sanctions for established violations but also investing in monitoring and analysis technologies capable of detecting and responding to misuse of data more effectively. On the other hand, analyzing the issue from a strictly national perspective is cursory. Greater international cooperation is crucial since the nature of AI and data transcends borders. Global collaboration could facilitate the creation of international standards that align data protection efforts worldwide. International treaties and the involvement and education of society as a whole about the implications of AI for privacy and data protection become essential tools. This includes educational initiatives and awareness-raising, as well as public participation channels in the legislative process. After all, data protection is not just a technical or legal issue but also a profoundly social and ethical matter.

Alexandre Barbosa da Silva and Ricardo Aronne prophesy the challenges of chaos, surrendering to the "minimal predictability of the future." To be more drastic, speaking of explainable and inexplicable AI, today it is no longer possible to perfectly understand the process of developing responses to many of the interactions obtained by these technological applications. It is a chaotic profile, therefore: it cannot be reconstructed, just as with the ship of Theseus. As this ship navigates this sea of chaos, Brazil's General Data Protection Law must evolve, not only to meet today's challenges but also to anticipate the complexities of tomorrow. The adequacy of the LGPD in the face of technological innovations will not be a definitive achievement but a continuous process of adaptation and learning. Only in this way can it be ensured that the protections offered by regulations are as dynamic and resilient as the technologies they aim to regulate. Legal professionals and norm creators, accustomed to static norms, must familiarize themselves with the Baumanian liquidity of the times, provoked by technology.

.

The adequacy of the LGPD in the face of technological innovations will be a continuous process of adaptation and learning.

Thiago Felipe S. Avanci *is a lawyer, holds a Ph.D. in Political and Economic Law, has a postdoctoral fellowship in Law and New Technologies, is an author of books, and is a university professor and researcher at*

Academic Coordinator Edison Spina

This article results from the author's investigation and analysis and does not necessarily reflect the opinion of CEST.