Digital Law in Brazil – Current Hot Topics | From Guidance to Active Oversight: Brazil's New Phase of Cybersecurity Regulation

The year 2025 marked a paradigm shift in Brazil's data protection landscape, as the National Data Protection Authority (ANPD) was elevated to the status of a regulatory agency, acquiring expanded powers of enforcement, rulemaking, and sanctioning. This institutional transformation inaugurates a new phase in the application of the General Data Protection Law (LGPD), in which the authority's previously advisory posture gives way to a more assertive and sanction-oriented approach. The Priority Topics Map for 2026–2027 and the updated Regulatory Agenda 2025–2026 reinforce this transition, making clear that security incidents will now be subject to proactive oversight and stricter penalties.

Under the LGPD, sanctions may include warnings with deadlines for corrective measures, simple or daily fines capped at 2% of a company's revenue up to fifty million reais per violation, public disclosure of infractions, partial suspension of database operations, or even prohibition of data processing activities. Resolutions No. 1/2021 and No. 4/2023 issued by the ANPD establish criteria for penalty application, taking into account severity, recurrence, and good faith. Furthermore, Resolution No. 15/2024 sets mandatory deadlines and procedures for reporting security incidents, requiring companies to notify breaches within three business days—or six days for small enterprises. Noncompliance results in fines and public disclosure, amplifying reputational damage.

In this context, both private and public organizations must be able to demonstrate concrete evidence of governance, risk management, and effective integration of technology with respect for fundamental rights. This entails implementing robust incident response plans, ensuring timely and transparent communication with the ANPD and affected data subjects, continuously monitoring regulatory publications, training technology, legal, and compliance teams, and mapping high-risk data processing operations—particularly those involving minors, sensitive data, or international transfers.

Controllers and processors are required to adopt technical and administrative measures to safeguard personal information, in accordance with Article 48 of the LGPD. In the event of an incident, they must assess the need to promptly notify the authority and affected individuals, describing the nature of the compromised data, the risks involved, and the mitigation measures adopted. The ANPD's Guidance Manual underscores that communication must be transparent and timely, under penalty of severe sanctions, including suspension of operations.

Minimum security standards for data processing are becoming increasingly critical. It is likely that the ANPD will mandate requirements such as encryption, vulnerability management, periodic audits, access controls, and rigorously tested

incident response plans. Crucially, organizations must demonstrate not only the formal adoption of such measures but also responsible decision-making and institutional maturity.

In summary, Brazil's regulatory environment for data protection is evolving rapidly. Organizations that comply with the LGPD and meet the requirements of the ANPD and other regulatory bodies will significantly reduce the risk of fines, operational disruptions, and reputational harm. Maintaining a proactive compliance posture is essential to ensuring legal certainty and competitiveness. The year 2026 demands that companies and public institutions be prepared for a more assertive ANPD, as its transformation into a full regulatory agency signals less tolerance and greater rigor in the oversight of cybersecurity incidents.

Cristiane Manzueto, partner at Montaury Pimenta, Machado & Vieira de Mello