TozziniFreire.

Cybernews

6th Edition | 2025

This is an informative newsletter
produced by the **Cybersecurity & Data Privacy**
practice of TozziniFreire Advogados.

INDEX

Click at the topic of your interest and browse through the content

EDITORIAL

In this edition of the Cybernews Bulletin, we highlight the main news on data protection in July 2025.

A recent study has revealed a 112% increase in court orders mentioning the Brazilian General Data Protection Law (LGPD in Portuguese) in Brazilian courts. The study indicates that the law is increasingly understood and applied by the Judicial Branch and citizens in the pursuit of their rights, reflecting a consolidation of the culture of personal data protection in Brazil.

Furthermore, the Ministry of Justice has formalized a recent Ordinance, published on June 30, 2025, authorizing the use of artificial intelligence (AI) with remote facial recognition in criminal investigations.

Also, the Superior Court of Justice (STJ in Portuguese) ruled that cryptocurrency platforms are liable for fraud in their systems, even when they use two-factor authentication. The decision was made after an investor had a loss with the improper transfer of bitcoins, and the Court understood that the failure in the platform's security justifies the platform's duty of compensating the investor.

Finally, the Brazilian Regional Appellate Labor Court of the 15th Region decided to prohibit the use of geolocation data to protect the privacy of the worker involved. The Court emphasized that the request for geolocation data could violate the plaintiff's privacy and delay the case without ensuring this data would actually be useful.

GENERAL NEWS

Decisions mentioning LGPD doubled in a year, as indicated by report

A recent study revealed a significant increase in court orders mentioning the Brazilian General Data Protection Law (LGPD) in Brazilian courts. Between October 2023 and October 2024, 15,921 decisions mentioning LGPD were identified, indicating a 112% growth compared to the previous period, which accounted for only 7,503 decisions. The report, prepared by the Center for Law, Internet and Society (Cedis-IDP) in partnership with Jusbrasil and with the support of the United Nations Development Program (UNDP Brazil), was presented at an-event taking place before the XIII Lisbon Forum.

According to Laura Schertel Mendes, director of Cedis-IDP, the data indicates the Judicial Branch has been applying LGPD in a more mature way. The legislation, which came into effect in 2020, has been increasingly understood and applied by citizens in pursuit of their rights. LGPD does not prohibit the use of personal data but regulates its governance and limits, which has become clearer over time.

In addition to the increasing number of references, the decisions mentioning LGPD are also more technically refined, revealing an evolution in the Judicial Branch's understanding of the application of the law. Also noteworthy is the shifting of the burden of proof in favor of data subjects, based on informational vulnerability, and the joint liability among data processing agents, topics that have also been more frequently addressed.

The outcome of the study reflects a consolidation of the culture of personal data protection in Brazil, which, in judicial processes, is no longer applied incidentally and has become a central part of the debate in decisions.

BACK TO INDEX

Ministry of Justice implements the use of artificial intelligence in criminal investigations

In an increasingly digital world, the recent Ordinance from the Ministry of Justice, published on June 30, 2025, has kept pace with technological evolution by authorizing the use of artificial intelligence (AI) with remote facial recognition in criminal investigations.

This Ordinance established clear guidelines that allow for using AI in specific situations, such as criminal investigations that are previously authorized by the Judicial Branch and lack other means of evidence; searches for missing persons or victims of crime; and the recapture of fugitive inmates. Moreover, this technology can be applied in cases of crimes with penalties exceeding two years, provided that the use is immediately communicated to the court authority.

It is important to highlight that, for other cases, the use of AI must be justified and analyzed regarding potential negative impacts, ensuring that its implementation respects legal principles and fundamental rights.

The main purpose of the Ordinance is to standardize procedures for the use of technology by federal and state public security agencies, aiming to ensure the protection of sensitive data and prevent unauthorized access.

Furthermore, this enables authorities to identify mobile devices in correctional facilities, allowing signals to be blocked, devices to be seized and data to be collected from seized electronic devices, under the Judicial Branch's supervision.

This new regulation demonstrates the Brazilian federal government's commitment to keeping up with technological innovations, aiming for effective results through the use of AI with due care for the protection of personal data.

STJ recognizes strict liability of cryptocurrency platform for security failure, even with two-factor authentication

In a unanimous decision, the Fourth Panel of the Superior Court of Justice (STJ) reaffirmed cryptocurrency investment platforms' strict liability for fraud that occurred in their systems, even when two-factor authentication is used. The judgment of Special Appeal No. 2,104,122/MG, reported by Justice Maria Isabel Gallotti, finished on May 20, 2025.

The case involved an investor who had his bitcoins improperly transferred – about 3.8 bitcoins, equivalent, at the time, to approximately R$ 200 thousand – although the transaction required login, password, PIN and confirmation by email. The platform claimed that the fault would lie exclusively with the user and third parties (hackers), a thesis accepted by the court of origin.

However, STJ reversed the decision, highlighting that the brokerage firm, as it is considered a financial institution — according to article 17 of Law No. 4,595/1964 and Precedent 479 of STJ — is strictly liable for fraud resulting from failures in its digital environment. The Court stressed that liability could only be disregarded if it was proven that the fault lied exclusively with the victim or third parties, which did not occur in the case.

The justice-rapporteur emphasized that the fraudulent transaction was completed with multiple layers of authentication, which evidences a failure in the company's security system. Thus, the duty to indemnify the investor for pecuniary damage and pain and suffering was recognized.

The decision reinforces STJ's authority on consumer protection in digital environments and imposes stricter responsibility on cryptocurrency platforms for the security of transactions.

BACK TO INDEX

TRT-15 dismisses digital evidence to protect worker's privacy

The Brazilian Regional Appellate Labor Court of the 15th Region decided to prohibit the use of geolocation data to protect the privacy of the worker involved. This decision was made following a disagreement between the parties regarding the previous ruling from the 6th Labor Court of Campinas, in the state of São Paulo.

The worker questioned the criteria used to calculate overtime, while the employer claimed there was denial of the right to be heard, particularly due to the refusal of using the worker's geolocation data as evidence.

The Court emphasized that the judge has the discretion to deny requests they deem unnecessary. In this case, the geolocation data was considered dispensable, as there was already sufficient evidence in the records. Furthermore, it concluded that the request for geolocation data could violate the plaintiff's privacy and delay the case without ensuring this data would be actually useful.

The ruling in this case demonstrated the Court's attention to the principles of data protection, especially the principles of purpose and necessity.

BACK TO INDEX

Cybersecurity in focus: growing risks, regulatory response, and the strategic role of legal governance

In an increasingly connected world, cybersecurity has transitioned from being a technical topic relegated to the backrooms of digital infrastructure to being a key element in institutional strategies, regulatory agendas, and the daily concerns of companies, governments, and citizens. The growing sophistication of cyberattacks, coupled with a high dependence on digital systems for critical services—such as healthcare, logistics, and finance—creates an atmosphere of constant vigilance, where failures in data protection can lead to severe and lasting impacts, from the operational, reputational and legal perspectives.

The recent case of C&M Software clearly illustrates this case. The technology company, which works as an integrator between financial institutions and the Central Bank, had its systems breached, resulting in the exposure of millions of records and personal data—including ID numbers, financial data, and bank transactions. The hacker attack, which may have involved the misapplication of R$ 500 million, is already considered the largest cyberattack in the history of the Brazilian financial system. The incident had immediate repercussions, not only due to the number of people affected but also because it involved a large chain of financial players, expanding the reach and complexity of the leak.

Another relevant aspect of this case is the suspicion that the attack may have been facilitated by an employee of C&M Software, who allegedly provided internal data and company credentials to the group of hackers, in exchange for money.

The Brazilian Data Protection Authority (ANPD in Portuguese) has been strengthening its institutional structure and strategic action to respond to internal information security challenges. In May 2025, the authority announced the creation of the Information Security Committee (CSIN in Portuguese) and the Cyber Incident Prevention, Handling, and Response Team (EPTIC in Portuguese). CSIN will focus on planning and creating internal cybersecurity guidelines, focusing on the protection of ANPD's informational assets, while EPTIC will take on a more technical and operational role, taking the lead in containing and analysing incidents, including intrusion attempts and integrity failures in databases under government management.

These initiatives are part of a broader plan of ANPD, reflected in its regulatory agenda for the 2025-2026 biennium. The agenda addresses various critical issues, including the regulation of Article 46 of the General Data Protection Law (LGPD), which mandates that data processing agents adopt security measures, both technical and administrative, capable of protecting personal data from unauthorized access and from accidents or unlawful destruction, loss, tampering, undue communication, or any form of inadequate or unlawful processing. Paragraph 1 of this article allows ANPD to set forth minimum technical standards related to these measures—a step that becomes increasingly urgent due to the growing number of incidents.

In 2021, the authority published an information security guide related to this topic for small data processing agents. The guide includes a checklist of security measures, and in April 2024, the Regulation on Security Incident Communication was published, establishing procedures for reporting incidents that could pose a risk or significant harm to data subjects. However, there is still room for further instructions on this matter, and future guidance from ANPD on this topic can be expected.

The inclusion of cybersecurity as a foundational part of ANPD's work is also consistent with the growing volume of notifications of security incidents. In the first half of 2025 alone, 217 reports of breaches were received, involving both the public and private sectors. Among these, attacks related to credential theft/social engineering and ransomware attack stand out.

In addition to the government body's initiatives aforementioned, the private sector plays a decisive role in the cybersecurity of companies and organizations in the sector. Cybersecurity should not be seen as a cost but as a strategic asset, directly linked to institutional reputation, to user trust, and to the legal viability of operations. The demand for security measures outlined in LGPD should not be limited to implementing firewalls or antivirus software, but should also encompass internal governance policies,

BACK TO INDEX

incident response plans, ongoing training, independent audits, and a security culture that permeates all levels of the organization.

However, the ideal cybersecurity scenario is not a reality for most part of the private sector yet. For example, a survey by the Federation of Industries of the State of São Paulo (Fiesp in Portuguese) revealed that, in the state, only 44.2% of respondent companies have a cybersecurity or information security organizational structure. Furthermore, 52.4% of these companies do not treat cybersecurity as a priority, despite recognizing it as necessary. The main challenges faced by companies in implementing LGPD are, according to the survey, training and awareness.

In times of accelerated digital transformation, sophisticated attacks, and increasingly vigilant regulation, the role of the legal sector goes far beyond post-incident litigation. Recent cases leave no doubt: it is essential to establish a solid and well-structured cybersecurity ecosystem while encouraging that all employees of companies align with this culture.

In this context, strengthening the culture of data protection and cybersecurity should be a transversal priority. The moment demands an active commitment from the public sector, the private sector, and civil society to building safer, more transparent, and accountable digital environments.

Partners responsible for the newsletter

- Patrícia Helena Marta Martins
- Marcela Waksman Ejnisman
- Carla do Couto Hellu Battilana
- Luiza Sato
- Bruna Borghi Tomé
- Sofia Kilmar
- Stephanie Consonni de Schryver