


# Cybernews.

---

2<sup>nd</sup> 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 

## 01 | Editorial

---

## 02 | Brazilian Legislation

---

/ANPD, LGPD and Discounts on Medications: Challenges for the Pharmaceutical Sector

## 03 | General News

---

/STJ: Government not required to compensate businesswoman for information leaked by government agents

/Internet service providers must provide user registration data

/STJ exempts bank from liability in “delivery boy scam”

# EDITORIAL

In this edition of Cybernews, we highlight the main news on data protection in February and March 2025.

Firstly, the 2<sup>nd</sup> Chamber of the Superior Court of Justice (STJ in Portuguese) upheld the decision rejecting the mental distress claim for R\$ 10 million made by a businesswoman who was arrested and alleged to have suffered excessive media exposure due to confidential information leaked by government agents.

Additionally, the 3<sup>rd</sup> Chamber determined that the IP address is sufficient for internet

connection providers to provide users' registration data, even without prior provision of a logical port (which allows the individualization and identification of users in cases of shared IP addresses) by internet application providers.

Finally, the 3<sup>rd</sup> Chamber also established the understanding that banks cannot be held liable for the "delivery boy scam" – in which third parties contact the victim, claiming that their card has been cloned and requesting that the consumer enter their password to unlock it – unless data leakage is proven.



# BRAZILIAN LEGISLATION

## ANPD, LGPD and Discounts on Medications: Challenges for the Pharmaceutical Sector

In March, the partners from the data protection practice area, Luiza Sato and Carla Battilana, visited the National Data Protection Authority (ANPD in Portuguese) to discuss current topics of interest to the market related to data protection. During the meeting, ANPD, represented by its director, emphasized the importance of several aspects that are fundamental for companies' compliance with the Brazilian General Data Protection Law (LGPD in Portuguese).

### Principles

Regarding the principles, one of the main points addressed was the importance of **transparency**. In practical terms, companies must always be clear and open about how they handle personal data, ensuring that data subjects are kept informed about how their information is being processed.

With respect to purpose, in the event of further processing of personal data, it is important that this be compatible with the original purposes communicated to the data subject, even if the new **purpose** is not identical.

### Compliance Practices

Additionally, it was highlighted the importance of companies structuring a **program for compliance** with the LGPD, implementing and adhering to a **data retention and deletion policy**, as well as preparing and maintaining, where appropriate, updated **Data Protection Impact Reports (RIPD)**, documenting data processing activities that involve risks and ready to be provided when requested by ANPD.

These measures are considered essential by ANPD for companies to demonstrate compliance with LGPD and, thus, to avoid penalties or at least serve as mitigating factors during an inspection process.

### Timeliness

Finally, ANPD stressed the **importance of companies responding to its information requests promptly**, as per Resolutions CD/ANPD No. 1/2021 and No. 4/2023. This is because any lack of response may be considered a violation of such norms and, consequently, be taken into account in defining any sanctions to be applied.

## **Technical Note ANPD No. 6/2025**

As imagined, failure to comply with these and other aspects may result in sanctions imposed by ANPD. Recently, this was observed in the case involving pharmacy chain RaiaDrogasil, the loyalty program Stix, and the Brazilian Federation of Associative and Independent Pharmacy Networks (Febrafar).

These entities were the subject of the Technical Note issued by ANPD's General Coordination of Inspection in February 2025, marking the **conclusion of an inspection process** initiated in May 2023, focused on **the processing of personal data by pharmacy chains and operators of loyalty and benefits programs**.

Delving deeper into the case, the investigation was launched to assess whether the practices adopted by these entities were compliant with LGPD. ANPD turned its attention to these practices due to concerns related to how **sensitive personal data**, especially health-related data, was being handled within **loyalty programs**, which often involve the personalization of offers and benefits based on **customers' consumption profiles**.

The points of concern raised by ANPD in its Technical Note highlighted three main concerns:

**I. Monetization of Health Data:** health data was being monetized for targeted advertising purposes without the necessary transparency or adequate legal basis, which could constitute a

deviation from the purposes originally communicated to data subjects.

**II. Biometric Data Collection:** the collection of biometric data — which also qualifies as a type of sensitive personal data — was occurring without considering less invasive alternatives that could meet the same purposes of authentication in loyalty programs, raising questions about the necessity and proportionality of processing such data.

**III. Clarity on Storage and Deletion:** the lack of clear information regarding data storage periods and procedures for personal data deletion was also identified as a failure, suggesting a possible violation of the necessity principle, as required by LGPD.

In response to the irregularities observed, ANPD imposed a series of specific preventive measures on the entities and initiated an Administrative Sanctioning Process against RaiaDrogasil to investigate potential irregularities involving personal data processing for purposes of forming behavioral profiles without the necessary legal basis.

Regarding the preventive measures, the authority determined that, among other things, RaiaDrogasil must implement **alternative methods of identity verification** for customers (that do not require biometric data), adopt transparency measures with data subjects (and with ANPD itself) about

personal data storage, and clarify to ANPD information about **how sensitive personal data is used to create behavioral profiles**. For Febrifar, the preventive measures include the need to implement **improvements in the communication** of privacy policies on the federation's website to **facilitate the exercise of rights by data subjects**.

Finally, the Technical Note reinforces the relevance of **strengthening transparency measures with data subjects**, which includes providing clear and accessible information about the purposes of processing their personal data, the storage period, and the procedures available for exercising their rights.

Regardless of whether the arguments presented by the audited agents were sufficient or whether some points raised by ANPD are open to discussion, the main message that remains, in line with the information obtained during the visit to ANPD in March, is the need to implement a robust compliance program and to conduct an appropriate impact assessment for data processing activities, especially when they involve sensitive data. These measures not only demonstrate companies' commitment to data protection but also serve as defense mechanisms against potential questioning and inspections.





# GENERAL NEWS

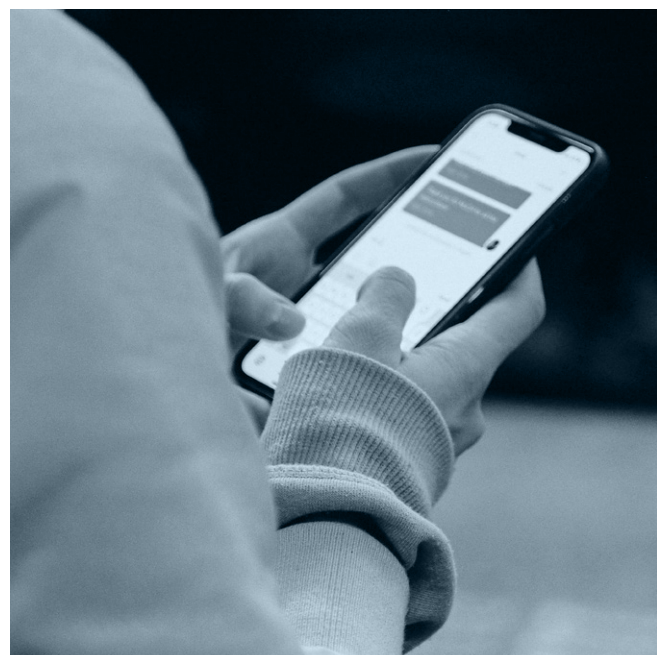
## **STJ: Government not required to compensate businesswoman for information leaked by government agents**

The 2<sup>nd</sup> Panel of the Superior Court of Justice (STJ in Portuguese) did not reconsider a mental distress claim against the Government made by a businesswoman involved in Operation Satiagraha, who claimed to have suffered excessive media exposure due to confidential information leaked by government agents.

The businesswoman requested R\$ 10 million in compensation, but the claim was deemed unfounded at first instance due to the lack of connection between the facts reported by the press and the alleged damages. The Regional Federal Court (TRF) of the 2<sup>nd</sup> Region upheld this decision, leading the businesswoman to appeal to STJ.

In her special appeal, the businesswoman argued that the TRF did not consider evidence regarding the unlawful conduct of government agents and new facts, such as the conviction of the operation's chief of police for breach of professional secrecy. However, the 2<sup>nd</sup> Panel of the STJ upheld the previous decision, denying the compensation.

In conclusion, the STJ's decision underscores the importance of a clear link between the actions of government agents and the alleged damages for the court to accept a mental distress claim due to the leak of confidential information. The fact that the court upheld that the claim is unfounded reflects not only the court's strictness in cases of data leaks but also the thorough analysis of evidence and the responsibility of the involved agencies.



## Internet service providers must provide user registration data

The 3<sup>rd</sup> Panel of the Superior Court of Justice (STJ) decided that an internet service provider must provide a user's registration data based solely on the indication of the IP address, without the need for a logical port.

The case involves Companhia Brasileira de Offshore (CBO), which sued Telefônica Brasil to obtain data about a user who sent an anonymous and defamatory email regarding salary differences.

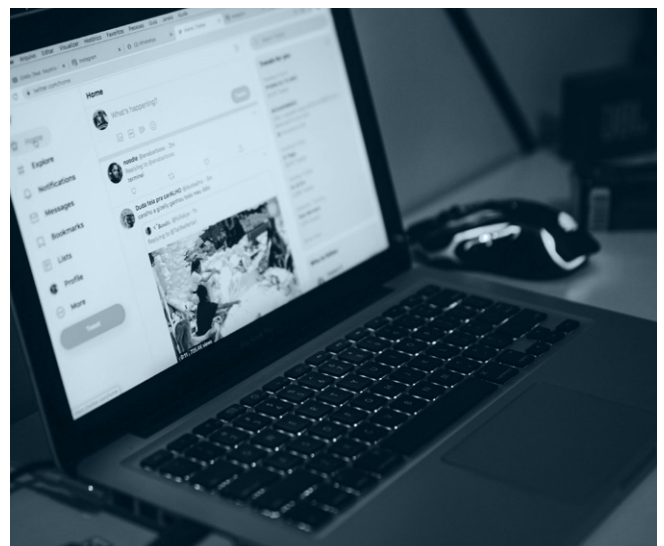
The trial and appellate courts of São Paulo Court (TJSP) ruled in favor of CBO, but Telefônica argued that it could not share the data due to confidentiality concerns as, without the logical port, providing information could involve disclosing data from hundreds of users sharing the same IP, who may not necessarily be connected to the facts in question.

At the STJ, Reporting Justice Nancy Andrighi ordered Telefônica to share the registration information, citing court precedents that require both connection and application providers to provide such data.

Telefônica defends its position to avoid exposing personal data of third parties, while CBO argues that the defamatory email harmed the reputation of those involved, and requests the user's full name, CPF (Individual Taxpayer ID Number), address, and phone number.

In her decision, the Justice noted that prior information about the logical port is not necessary for the connection provider to make the user's data available, as the provider is required to store and provide the IP and logical port (Special Appeal 2170872). The Panel had previously stated that the Internet Civil Framework establishes the obligation to store and provide information about the originating logical port (Special Appeal 1777769) and that this must be stored until the lawsuit for award of damages is barred by the statute of limitations, according to the Civil Code (Special Appeal 1622483).

Thus, the STJ's decision reaffirms the responsibility of internet service providers to facilitate the identification of users involved in unlawful conduct, balancing the protection of personal information with the need for justice in defamation cases.





## STJ exempts bank from liability in “delivery boy scam”

The Superior Court of Justice (STJ) ruled that a bank cannot be held liable for the “delivery boy scam” in the absence of evidence of data leakage, even in cases involving a consumer in a state of hyper-vulnerability. This decision was made by a majority of votes by the 3rd Panel.

In the “delivery boy scam,” scammers impersonate representatives of financial institutions and inform the customer that their card has been cloned, asking for a delivery boy to collect the card in person. They also request that the customer enter their password on the cell phone before the delivery.

In this specific case, the consumer, who was undergoing chemotherapy for cancer treatment, was deceived by scammers who convinced her to install a program that allowed remote access to her computer. She also provided her banking details and passwords, enabling fraudulent transfers.

The Court of Justice of Minas Gerais (TJMG in Portuguese) concluded that the bank could not be held liable for purchases made using the password, as the consumer voluntarily provided her personal information to the scammer, even though she was a victim of fraud.

The trial at the STJ began in December 2024 and was concluded in February this year, with Justice Nancy Andrighi as the rapporteur. She defended the bank’s strict liability in accordance with STJ Precedent 479, which

states that financial institutions are liable for damages resulting from frauds and crimes committed by third parties in banking operations. The rapporteur was supported by Justice Humberto Martins, but her position did not prevail.

Justice Ricardo Villas Bôas Cueva dissented, arguing that there was no failure in the service provided by the bank. He argued that the scammers acted cunningly, using only the victim’s registration data. Cueva also highlighted that the difficulties arising from cancer treatment do not mitigate the consumer’s responsibility. Justices Moura Ribeiro and Antônio Carlos Ferreira supported Cueva’s position, forming the majority.

There are precedents in private law panels that exempt banks from liability when the consumer hands over their password to scammers. In February, the 4th Panel upheld a decision from a state court that found no failure in service in operations regularly conducted, in which the account was accessed with the card and password provided to a third party by the account holder before the fraud was reported (AREsp 2756405).

However, this issue requires ongoing monitoring, as this understanding may change, and banks could be held liable in cases involving alleged data leakage and atypical transactions and hyper-vulnerable consumers.



## Partners responsible for the newsletter

- ⑧ Patrícia Helena Marta Martins
- ⑧ Marcela Waksman Ejnisman
- ⑧ Carla do Couto Hellu Battilana
- ⑧ Luiza Sato
- ⑧ Bruna Borghi Tomé
- ⑧ Sofia Kilmar
- ⑧ Stephanie Consonni de Schryver