

**TozziniFreire.**


# Cybernews

---

11<sup>th</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 GENERAL NEWS

---

**ANPD launches Inspection Panel and expands transparency on its regulatory performance**

**STJ: Compensation for data sharing requires proof of damage**

**Judge authorizes AI petition platform, imposes user notice, and highlights importance of personal data protection**

**Possible massive leak of court data at the Regional Federal Appellate Court of the 4th Region is under investigation by the Federal Police**

# EDITORIAL

---

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

Firstly, the National Data Protection Agency (ANPD) launched an Inspection Panel and expanded transparency about its regulatory activities.

Also, the STJ ruled that improper data sharing only gives rise to compensation if there is proof of actual disclosure and concrete damage. In the case in question, since the consumer failed to demonstrate the occurrence of damage, the compensation claim was denied. The 4th Panel's decision differs from the 3rd Panel's understanding, which holds that unauthorized data sharing entails presumed moral damages.

In addition, Federal Judge Jhonny Kenji Kato, from the 27th Federal Court of Rio de Janeiro, has authorized the continued operation of the "Resolve Juizado" platform, which uses artificial intelligence to automate the drafting of petitions, highlighting that the platform does not work as legal consulting. Despite concerns raised by the Brazilian Bar Association (OAB/RJ) regarding professional ethics, the judge required clear notices about the service's limitations and emphasized the need for personal data protection, determining that user information should be processed securely and transparently.

Finally, São Paulo Bar Association requested the Federal Police to investigate a possible mass leak of data from court cases at the Regional Federal Appellate Court of the 4th Region.

# GENERAL NEWS

## ANPD launches Inspection Panel and expands transparency on its regulatory performance

In November this year, the **National Data Protection Agency (ANPD) launched its new Inspection Panel** (available in Brazilian Portuguese at this [link](#)), an interactive tool aimed at facilitating public access to information related to inspection actions conducted by the Agency. In addition to reinforcing the institutional commitment to transparency and accountability, this tool allows companies, researchers and other interested parties to understand more clearly the progress of the (i) inspection processes, (ii) conducts investigated and (iii) priority topics monitored by the Agency.

**The Panel presents consolidated and dynamic data on inspection procedures, preparatory processes and administrative sanctioning processes.** Evidenced information includes the total number of lawsuits filed per year, the most impacted sectors, the estimated ranges of affected data subjects, and recurring topics of investigation (such as sensitive data processing, facial recognition, security incidents, and improper marketing of data).

According to the last update until the closing of this newsletter (dated November 6th), 63 inspection processes have been initiated, and there are already 12 sanctioning processes, 8 of which have been completed and 4 are in progress.

In addition, the tool allows you to view the average decision time, the nature of the sanctions applied, and the details of the conducts analyzed under specific articles of LGPD (Brazilian Data Protection Law). In this regard, the Panel offers a comprehensive view of ANPD's performance patterns and the regulatory trends that are expected to guide the market in the coming years.

It is also worth noting that publicly providing these statistics is in line with the Biennial Monitoring Cycle, provided for in ANPD Resolution No. 10/2023, whose first cycle was completed in the first half of 2025 and is expected to resume now in 2026. In this scenario, the Panel translates the results of this systematic monitoring into concrete data,

allowing us to observe the evolution of the topics inspected and the Agency's maturity in exercising its regulatory functions. It is clear, therefore, that **the Panel works as an important indicator of areas that tend to receive greater attention from ANPD over the next cycles.**

In this context, it is important to highlight that the practical effects of this cycle have already been noted by the market. Specifically, in the last few months, **the Agency has sent letters to companies in various sectors requesting clarification on compliance with their transparency practices**, especially regarding the availability of the DPO's contact details, the existence of channels accessible to data subjects, and the clarity of information related to international data transfer operations.

This move, in turn, highlights the **importance of keeping Privacy Policies up to date**, complete and in line with the applicable regulatory requirements in order to reduce the risk of questioning by ANPD. In addition, reviewing these transparency instruments became an immediate measure to ensure compliance with ANPD's expectations identified throughout the monitoring process.

From a strategic standpoint, the launch of the Panel and the advancement of ANPD'S

Monitoring Cycle highlight the relevance of continuous adaptation by organizations, which should implement strategies such as developing structural projects for compliance with LGPD, raising team awareness initiatives and adopting routine practices for reviewing and updating policies, records, and internal flows.

As such, the consolidation of a data protection culture, supported by consistent preventive mechanisms, is increasingly crucial to mitigate risks, respond efficiently to ANPD's requirements and strengthen the trust of users, partners and other stakeholders.





STJ: Compensation for data sharing requires proof of damage

The Superior Court of Justice (STJ in Portuguese) ruled that for a consumer to receive compensation for the improper sharing of their personal data, it is essential to prove that information has been actually disclosed and that damage has occurred. In the case in question, the consumer claimed that their data was sold without authorization by a credit score platform, seeking compensation for moral damages due to the exposure of personal information such as name and CPF (Individual Taxpayer ID Number).

At the lower court, the judge acknowledged excessive data processing and ordered the deletion of the information but denied the compensation claim, for lack of concrete evidence of confidential data disclosure. São Paulo Court of Justice (TJSP) reversed the ruling only to revoke the deletion of data.

In the STJ, the judge-rapporteur, Maria Isabel Gallotti, from the 4th Panel, reaffirmed that under the General Data Protection Law (LGPD), personal data can be processed for credit protection, and that merely sharing information does not automatically result in moral damage. The judge emphasized the consumer needs to demonstrate the illegality of the disclosure and the resulting negative

impact. Consequently, the action was found invalid, and compensation to the consumer was denied.

This STJ decision highlights a divergence of understanding at the Superior Courts since the 3rd Panel recognizes that mere unauthorized data sharing generates presumed moral damage. This scenario underscores the importance of continuously monitoring the Court's decisions for the development of case law in personal data protection.



## Judge authorizes AI petition platform, imposes user notice, and highlights importance of personal data protection

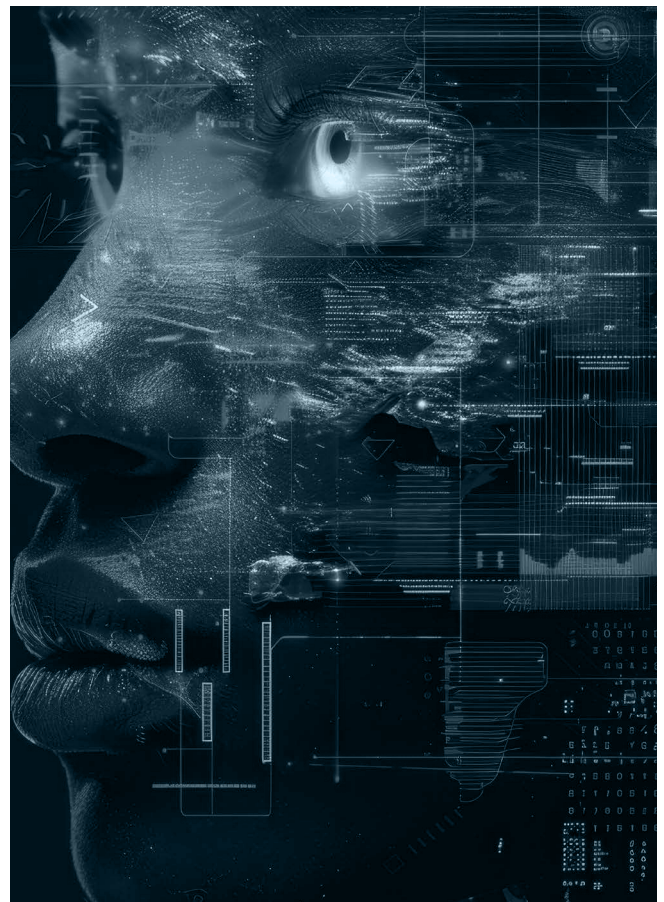
Federal Judge Jhonny Kenji Kato, from the 27th Federal Court of Rio de Janeiro, decided to keep the operation of the “Resolve Juizado” platform, which allows the automated drafting of initial petitions for Special Courts. The ruling was based on the conclusion that the platform’s activities do not constitute legal consulting or the exclusive practice of law.

The action was brought by the Brazilian Bar Association – Rio de Janeiro Section (OAB/RJ), which argued that the use of artificial intelligence (AI) to generate petitions could compromise professional ethics and trivialize the practice of law, leading to poorly evidenced actions and overburdening the Judiciary Branch. However, the judge found that “Resolve Juizado” functions as an automated tool that organizes and formats information provided by users without conducting legal analysis or offering advice.

While allowing the platform to continue its services, the judge required that clear notices be included informing users that:

- It does not offer legal consulting, advisory services, or guidance;

- There is no lawyer responsible for the content of the petitions;
- The service is limited to text automation without technical analysis;
- Content generated by artificial intelligence may have inaccuracies or biases.



These notices must be prominently displayed on the website's homepage and before any document is generated, ensuring that users understand the limitations of the service.

The ruling also underscores the significance of personal data protection, establishing that all user information should be processed securely and transparently to mitigate risks such as misuse or privacy violations. The judge further ordered the defendant to prove, within 30 days, that they have adopted the necessary measures to comply with the information obligations and to adequately adjust advertising materials, under penalty of a BLR 5,000 fine for non-compliance.

The innovation in access to justice was another highlighted aspect, particularly for users facing literacy and textual organization challenges. The judge stressed that the judicial system's overload is a result of structural factors, not the use of technology.

This ruling marks a significant milestone for technology in the legal field, balancing the protection of legal prerogatives with the need for modernization and innovation in the court system. Simultaneously, it reinforces the importance of protecting personal data in this new context, ensuring that users' information is managed appropriately while scrutinizing companies' practices that provide automated services to prevent ethical breaches in the legal profession.





## Possible massive leak of court data at the Regional Federal Appellate Court of the 4<sup>th</sup> Region is under investigation by the Federal Police

The Brazilian Bar Association – São Paulo Chapter (OAB-SP) filed a criminal complaint with the Federal Police requesting an investigation into a security incident involving the electronic case management system of the Regional Federal Appellate Court of the 4th Region (e-PROC).

According to the report, there was large-scale automated and unauthorized access using the credentials of a lawyer whose identity has not been revealed. It is estimated that between 50,000 and 200,000 cases have been improperly accessed, with the potential exposure of sensitive data of up to 400,000 individuals, including lawyers, litigants, witnesses, and public servants.

The TRF-4 itself identified patterns of “massive and robotic” queries, characterizing suspicious activity. The complaint points out that, in the first three days of

September, approximately 260 requests per minute were recorded, totaling about 200,000 automatic queries.

The connections originated from IP addresses linked to an international provider based in India, associated with VPN services and anonymous proxies, evidencing a deliberate attempt to mask the origin of the accesses. Nevertheless, some of the IPs were geolocated in Brazil, specifically in the states of São Paulo and Minas Gerais.

This episode reinforces the growing vulnerability of electronic court systems to sophisticated cyberattacks and the need for robust strategies for digital governance, regulatory compliance, and incident response.



## Partners responsible for the newsletter

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