TozziniFreire.

Cybernews

1st Edition | 2026

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 Cybernews Newsletter, we highlight the main news on data protection debates in January 2026.

Firstly, Brazilian notary public offices launched the e-Not Provas tool, which allows digital content, such as social media posts and messages in apps, to be recorded, granting them legal validity. Under the supervision of notaries public, the service ensures the integrity of evidence in a secure environment, meeting growing demands in the digital context. The initiative modernizes the legal field, enabling the use of digital evidence in court and administrative proceedings.

Recently, the Superior Labor Court (TST) ruled that geolocation can be used as digital evidence in labor claims involving requests for overtime pay, provided it complies with privacy and confidentiality limits.

In addition, earlier this year, Justice Alexandre de Moraes of the Brazilian Federal Supreme Court (STF) opened an investigation into a possible leak of data from Court justices, originating from the Federal Revenue Office and the Brazilian Financial Control Council (Coaf).

Furthermore, the Consumer Defense Institute (Idec) filed a complaint against Grok tool, an artificial intelligence from platform X, to the Brazilian Data Protection Agency (ANPD) for modifying images of real people, including children, in a sexualized manner and without consent.

Finally, Airbnb Digital Platform Ltd. was ordered to pay BRL 6,000 as non-pecuniary damages as a result from the break-in by a third party in an apartment rented through the platform.

Finally, please check the Priority Topics Map for 2026-2027 and the updates on ANPD's 2025-2026 Regulatory Agenda.

GENERAL NEWS

Notary public offices launch new platform "e-Not Provas"

Notary public offices have recently launched the innovative tool e-Not Provas, which revolutionizes how evidence on content available on the internet is currently handled.

The e-Not Provas tool offers a digital service that allows information published on websites, messages exchanged in apps, and posts on social media to be recorded, granting legal validity to this content. With a notary public present, responsible for ensuring public trust, the integrity of the information recorded is guaranteed in a controlled virtual environment, preventing any alteration or external interference during evidence collection. This aspect is crucial, as it ensures that the authenticity of the evidence be preserved over time.

In the information era, where disputes and litigation often revolve around virtual elements, the role of e-Not Provas becomes even more evident. This tool serves not only individuals, but also companies and legal professionals who need to validate the existence and presentation of certain content at specific times. Evidence is collected in an isolated and secure environment, where user privacy is respected and protected.

In addition to technical innovation, the tool generates cryptographic hash codes, which guarantee evidence integrity, reinforcing that the material produced is reliable.

At affordable prices, which correspond to notarial authentication fees, and storage for up to five years, this tool is an agile and effective response to the needs of demands requiring an interface between the Law and evolving technologies.

TST allows the use of geolocation in labor cases for calculation of overtime

The Superior Labor Court (TST in Portuguese) has decided that companies can use geolocation data – technology that identifies a person's geographic location through GPS, Wi-Fi or mobile networks – as evidence in labor lawsuits involving overtime claims.

In the two cases analyzed, one involving a sales representative and the other, a bank employee, TST concluded that geolocation is a valid means to verify working hours, provided that privacy and confidentiality limits are respected.

The decision was made by the Subsection II Specialized in Employment Disputes and by the 5th Panel of the TST, which considered the aforementioned evidence to be precise, necessary and proportional, in accordance with the provisions of the General Data Protection Law (LGPD in Portuguese) and the Brazilian Civil Rights Framework for the Internet (MCI). Both laws allow the use of personal data in the regular exercise of rights in court cases.

The court also noted that geolocation in such cases does not violate the fundamental right to privacy, established by the Federal Constitution. It should be emphasized, however, that its use must be strictly limited to the employment contract period and the schedules claimed by the employee. Additionally, cases that rely on this mechanism must be closed to the public to ensure protection of confidential information.

According to the TST, when used appropriately, geolocation does not violate the privacy or telematic secrecy of employees, representing a significant advancement in accepting digital evidence in labor disputes.

Justice Alexandre de Moraes opens investigation into leak of data from Supreme Court justices

In January 2026, Brazil witnessed an event underscoring the importance of personal data protection: justice Alexandre de Moraes of the Federal Supreme Court (STF in Portuguese) launched an investigation into a potential leak of data concerning Court ministers, sourced from the Federal Revenue Office and the Brazilian Financial Control Council (Coaf in Portuguese). This case involves allegations of irregular breach of tax confidentiality, raising critical questions about the responsibilities associated with the use of sensitive information.

The General Data Protection Law (LGPD in Portuguese) in Brazil requires that personal data be processed transparently and with the necessary consent. Access by the Federal Revenue Office and Coaf to such information requires court authorization, particularly in light of the privacy concerns of those involved, including the justices' family members.

The investigation, which will be conducted by the Federal Police, emphasizes the need for stringent controls over the use of protected information to prevent irreparable harm. The responsibility of governmental institutions in safeguarding the data they manage must be prioritized, especially in investigations with political and social ramifications.

Moreover, private sector entities are also required to adopt effective data governance practices to ensure compliance with current regulations. This includes regular audits and training on data privacy.

The STF investigation serves as a reminder of the central role of data protection in the digital age. It is imperative that all stakeholders — individuals and institutions — implement robust practices to ensure legal compliance and respect for fundamental rights. Transparency and security in information management are essential for maintaining public trust.

Idec files complaint against Grok with ANPD due to sexualized modification of images portraying real people

On January 14th, 2026, the Brazilian Consumer Protection Institute (Idec in Portuguese) filed a complaint with the Brazilian Data Protection Agency (ANPD) requesting an investigation into Grok – artificial intelligence tool integrated into the *X* platform – and the adoption of restrictive measures throughout the country.

According to Idec, Grok has repeatedly violated LGPD, by generating sexualized images which preserve real characteristics of the portrayed people, including children and teenagers, without consent. Users were prompting the AI tool to alter photos of real people, in order to generate images of them fully undressed or in revealing clothing.

Among other requests, the institute seeks the immediate suspension of all Grok features related to personal data processing. Idec also requests that ANPD investigate the violations, implement urgent measures to prevent or repair serious damage, and summon *X* representatives to provide clarifications.

The institute also points out that the generation of this type of content by Grok has been subjected to investigations and sanctions by authorities in California, the European Union, the United Kingdom, and India, among other jurisdictions, as it is a "*systemic and global*" problem.

On the same date, *X* announced the adoption of measures to block, in certain jurisdictions, Grok's ability to modify photos and generate images of people wearing "*bikinis, underwear, and other similar items*."

The episode highlights the constant tension between the advancement of AI technologies and the need to safeguard rights guaranteed by the Brazilian legal system, such as data protection, child protection, and the inviolability of privacy, honor, and image.

Same password: Airbnb will be liable for damages for third party entering rented apartment

The 1st Panel of the Special Courts of Paraná's Court of Justice (TJ-PR in Portuguese) ordered Airbnb Plataforma Digital Ltda. to pay BRL 6,000 as non-pecuniary damages due to a third-party invasion of an apartment rented through the platform.

The incident occurred when two guests booked an apartment through Airbnb, and on the second day of their stay, a stranger accessed the property using the electronic lock. Upon reporting the situation to the host, the guests were informed that there had been a mix-up regarding the apartment number reserved, as the host also rented another unit in the same building.

Although the trial court has dismissed the mental distress claim, TJ-PR overturned this decision upon reviewing the case. The rapporteur, judge Douglas Marcel Peres, rejected the host's justification, emphasizing that using a single password for different units in the same building jeopardizes the safety and privacy of guests.

The judge highlighted that someone's fundamental expectation when booking accommodation is the assurance of safety on the premises and he reported the single password practice as a clear risk for unauthorized access by third parties.

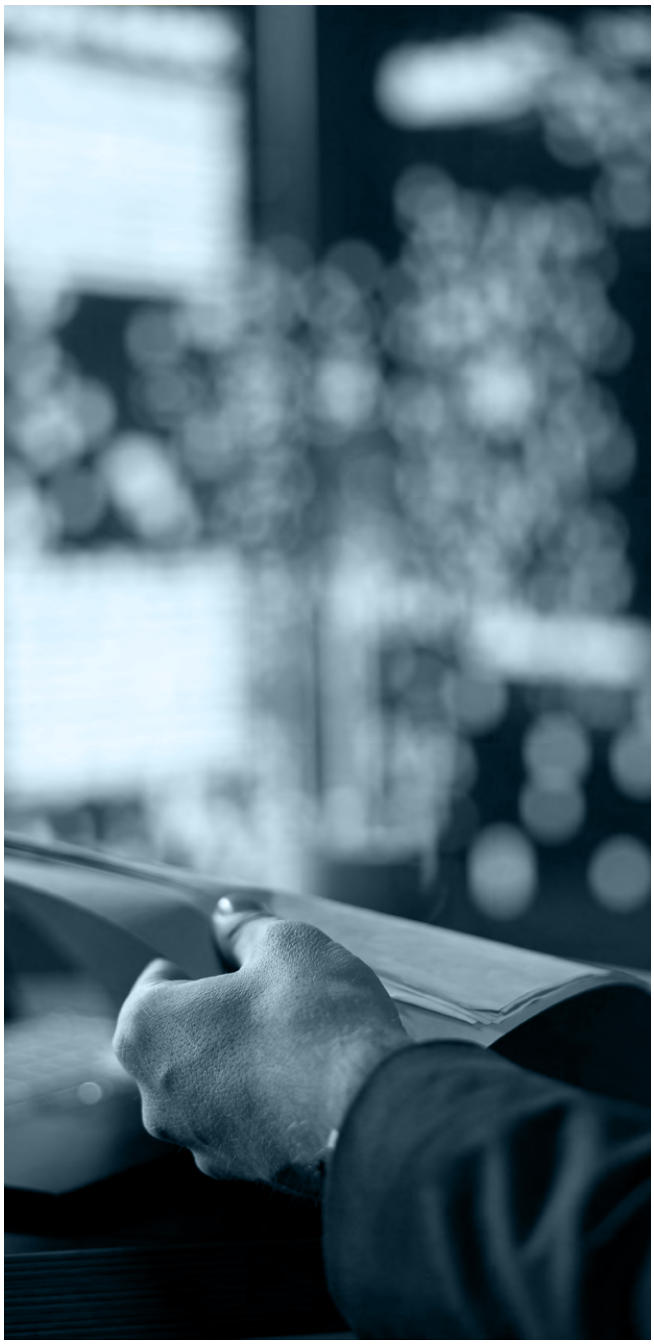
In conclusion, this case underscores the critical need for robust data protection and privacy measures on digital platforms.

The expectation of safety is paramount for consumers, and service providers must implement effective security protocols to safeguard user information and property.

Discussing privacy and data protection, especially in incidents like this, is essential for building trust in the sharing economy and ensuring the safety of everyone involved.

ANPD IN FOCUS

ANPD's Priority Topics Map for 2026-2027 and update of 2025-2026 Regulatory Agenda



On December 24th, 2025, the Brazilian Data Protection Agency (ANPD) published two resolutions guiding its actions for the upcoming cycles: Resolution CD/ANPD No. 30/2025 (please read it here), which defines the Priority Topics Map on Inspection for 2026-2027, and Resolution CD/ANPD No. 31/2025 (please read it here), which updates the Regulatory Agenda for 2025-2026.

The joint publication of these resolutions reinforces an **integrated strategy for regulation and inspection**, which will involve ANPD's monitoring, guidance, and preventive actions on matters related to data protection and Law No. 15,211/2025 (Brazilian Digital Statute for Children and Adolescent or ECA Digital).

See below a summary of the main topics presented in ANPD's Priority Topics Map and Regulatory Agenda:


1st semester/2026
2nd semester/2026
1st semester/2027
2nd semester/2027
Regulation
AI: 20 inspections on emerging technologies, especially AI systems
Processing by the Government: +20 inspections on compliance by the Government
Protection of children and adolescents in the digital environment: +30 inspections on compliance with the requirements of ECA Digital
Data subjects' rights: 10 inspections related to biometric, health or financial data
Data subjects' rights: 25 inspections on different topics + 5 inspections on secondary use of data for advertising
Inspection
1. Data subjects' rights
2. DPIA
3. Data sharing by the Government
4. Biometric data
5. Security measures
6. IA
7. Anonymization and pseudonymization
1. Aggregators of personal data
2. Health data
3. Guidance on the scope and general obligations of ECA Digital (providers of IT products or services)
4. Inspection and Sanction of ECA Digital - Review of Resolutions CD/ANPD No. 1/2021 and No. 4/2023
5. Age verification mechanisms
1. Normative process within the scope of ANPD: revision of Ordinance No. 16/2021
1. Rules on good practice and governance
2. Legal hypothesis of consent and credit protection

The **Priority Topics Map** establishes four priority themes for ANPD's inspection activities during 2026-2027, each with specific goals and biannual schedules:

i. Data subjects' rights, particularly regarding the processing of biometric, health, and financial data;

ii. Protection of children and adolescents in the digital environment;

iii. Processing of personal data by the government; and

iv. Artificial intelligence and emerging technologies related to personal data processing.

ANPD defined these topics by analyzing information from requests, incident reports, and inspection actions over the last two years.

ANPD updated the 2025-2026 Regulatory Agenda to include new items related to ECA Digital, make cross-cutting normative improvements, and maintain previously planned topics:

i. Mechanisms for age verification;

ii. Guidance on the scope and general obligations of ECA Digital for IT product or service providers; and

iii. Review of sanctioning resolutions No. 1/2021 and No. 4/2023 in light of ECA Digital.

For the private sector, the trend is toward intensified enforcement of data subjects' rights, particularly concerning children and adolescents, sensitive data (biometric, health, and financial data), targeted advertising based on secondary data use and measures for compliance with ECA Digital, which will require revisions to legal bases, data minimization, and data governance. In the **Artificial Intelligence** field, regulatory developments and compliance testing are expected, focusing on automated decisions and risks to vulnerable groups.

In the public sector, 2027 will feature a cycle of 20 inspections and monitoring of shared personal data usage, driving compliance with technical and legal safeguards.

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