TozziniFreire.

Cybernews

2st 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

01 EDITORIAL

02 GENERAL NEWS

The Grok case and the new challenges of artificial intelligence regulation in Brazil

STF Proposes Task Force to Identify Deepfakes in the 2026 Elections

Small-Claims Court Decides to Compensate Driver for Personal Data Used in Fraudulent Registration

TSE Prohibits Smart Glasses in Voting Booths for the 2026 Elections

EDITORIAL

In this edition of the Cybernews Newsletter, we highlight the main news about the data protection debate in Courts for February 2026.

Firstly, check out the Grok case and the new challenges on the artificial intelligence regulation in Brazil.

Also note that the Federal Supreme Court (STF in Portuguese) proposed creating a task force to identify deepfakes in the 2026 elections. Justice Gilmar Mendes emphasized that the confusion between true and false information threatens democratic integrity. The technical team will consist of specialists and research centers, with a regulatory framework on the use of AI focusing on the transparency of digital platforms. Mendes also pointed out the importance of partnerships between the Superior Electoral Court (TSE in Portuguese), the National Data Protection Authority (ANPD in Portuguese), and technology companies to improve detection and surveillance. The public hearings aim to gather inputs for electoral guidelines in a rapidly evolving technological environment.

Additionally, a Small-claims Court of the Federal District ruled that company 99 must compensate a driver who could not work after his data was used in a fraudulent registration on the platform.

Finally, the TSE banned the use of smart glasses in voting booths for the 2026 elections. A draft resolution reinforced that wearable devices with cameras or connections are incompatible with the secrecy of the voting process.

GENERAL NEWS

The Grok case and the new challenges of artificial intelligence regulation in Brazil

The beginning of 2026 was marked by intense debates about the ethical and legal limits of generative artificial intelligence. **The case of Grok, a chatbot developed by xAI and integrated with social media X, has raised questions about governance, privacy, and digital security, especially in the face of incidents involving the generation and dissemination of images created by artificial intelligence without consent**.

Grok uses generative language and image models to answer questions and create visual content from text commands. Unlike other platforms, the tool stood out for adopting a more permissive moderation policy, which would have enabled the circulation of sexualized and non-consensual images of women, children, and adolescents, known as deepfakes. According to investigations released by the international press, millions of images of this type were generated in a few hours, raising concerns among authorities, experts and digital rights organizations.

In Brazil, the repercussion led the Brazilian Institute for Consumer Protection (Idec in Portuguese) to file a formal complaint with the National Data Protection Agency (ANPD in Portuguese), asking the service to be immediately suspended in the country. At the same time, the National Consumer Secretariat (Senacon) and the Federal Prosecution Office (MPF) issued recommendations to xAI, requesting the implementation of technical measures to identify, review, and remove inappropriate content, as well as the deletion of accounts linked to its production. Authorities pointed out possible violations of the Brazilian General Data Protection Law (Law No. 13,709/2018), the Brazilian Consumer Protection Code (Law No. 8,078/1990), the Child and Adolescent Statute (Law No. 8,069/1990) and the Brazilian Civil Rights Framework for the Internet (Law No. 12,965/2014).

The entities also stressed the need for effective moderation and algorithmic governance mechanisms, capable of preventing the reproduction of potentially illicit or abusive content. In response, xAI announced temporary restrictions on the use of the tool, limiting the image generation functionality.

Internationally, the repercussion was also significant. The European Commission imposed a provisional measure on X in the context of the Digital Services Act (DSA), determining the preservation of internal documents about Grok until the end of 2026. Governments in the United Kingdom, France, India, and Malaysia have also adopted similar measures, by launching investigations and establishing restrictions on the use of Grok, reinforcing the global trend of strengthening the regulation on artificial intelligence, with a focus on mitigating risks related to content generated by automated systems.

These developments occur in parallel with the legislative process, in Brazil, concerning Bill No. 2,338/2023, whose goal is to establish a regulatory framework for artificial intelligence, and in light of the Brazilian "Digital ECA," which aims to strengthen protections for children and adolescents in digital spaces. The proposal provides for principles of transparency, security and accountability in the development and use of technology, as well as risk assessment and auditing mechanisms. The debate around Grok highlights the practical importance of these discussions, especially to establish duties of control, response, and redress in cases involving generative technologies.

The Grok case illustrates the complexity of regulatory challenges related to artificial intelligence and reinforces the importance of cooperation between data protection agencies, consumer protection, and the Prosecution Office. The measures adopted in Brazil and abroad demonstrate the efforts to balance freedom of innovation and protection of fundamental rights, promoting the ethical and safe use of technology.

For the private sector, **the episode reinforces the relevance of AI compliance policies, impact assessments, and algorithmic governance internal mechanisms, as key elements to ensure compliance and trust in a rapidly evolving regulatory environment. From an economic perspective, well-conducted prior assessments reduce the risk of wasted investments and rework by preventing products from being launched only to later be taken offline or significantly restructured due to regulatory non-compliance**.

STF Proposes Task Force to Identify Deepfakes in the 2026 Elections

During the opening of the public hearings at the Superior Electoral Court (TSE), Justice Gilmar Mendes of the Federal Supreme Court (STF) advocated for the creation of a specialized task force to identify content produced by artificial intelligence (AI), particularly deepfakes, in the context of elections.

The justice highlighted that the difficulty for voters in distinguishing between authentic and tampered data poses a threat to the integrity of the democratic process. The proposal envisions a technical team composed of experts and research centers focused on quickly detecting such content and on information security.

Additionally, he also advocated for a proactive regulatory framework regarding the use of AI, to be implemented in 2024, emphasizing transparency and the duty of care for digital platforms. Using deepfakes is already prohibited by electoral legislation, but the justice underscored the importance of partnerships between the TSE, the National Data Protection Agency (ANPD), and technology companies to enhance prevention and surveillance.

The public hearings aim to gather inputs for the rules governing the 2026 elections in a landscape of rapid technological transformations and growing challenges to data protection and voter trust.

Small-Claims Court Decides to Compensate Driver for Personal Data Used in Fraudulent Registration

In a ruling handed down by the Small-claims Court of Samambaia/DF, a driver whose data was used fraudulently on the 99 platform will be granted R$ 3,000 as non-pecuniary damages.

The judgment ordering the payment was based on the recognition of a consumer relationship by analogy and the company's strict liability.

The case began when the driver, while attempting to register with 99 POP, discovered that his data was being misused. With records of fraudulent rides, unknown bank account details, and access from various locations, the situation negatively affected his professional activity and put his identity at risk.

In the lawsuit, the driver argued that there was a failure in the platform's digital security and violation of the General Data Protection Law (LGPD in Portuguese).

In its defense, the company argued that its activities were limited to software licensing and that the Consumer Protection Code (CDC in Portuguese) did not apply to the case. However, the judge considered that the lack of necessary precautions to prevent the misuse of the driver's data was a serious mistake on the part of the company.

The decision emphasized that 99, by operating in a segment that deals with personal data and technology, assumes the risk of incidents and must bear the consequences of its failures. The judge recognized the consumer relationship by analogy and the lack of evidence to support the company's argument regarding the legality of the fraudulent registration.

Thus, the decision demonstrated the importance of adopting a robust verification and security system for technology platforms to ensure not only consumer's trust but also the viability of the platforms in the market.

TSE Prohibits Smart Glasses in Voting Booths for the 2026 Elections

The Superior Electoral Court (TSE) has decided to prohibit the use of smart glasses in voting booths during the 2026 elections, reinforcing the incompatibility of these devices with the secrecy of the voting process.

This decision was motivated by the increasing use of technologies that allow for real-time recording and transmission of images, which pose a direct risk to the privacy of voters.

The prohibition is already outlined in the sole paragraph of Article 91-A of Law No. 9,504/1997, which forbids the possession of cell phones, cameras, and camcorders in the voting booths. Consequently, the TSE has updated the guidelines in the draft of the General Acts of the Electoral Process, specifying that the possession of radiocommunication equipment or any instrument that could compromise the secrecy of voting is also prohibited, even if turned off.

Moreover, the draft clarifies that all devices that allow, in any way, for the recording or disclosure of votes fall under this restrictive category.

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