

TozziniFreire.
ADVOGADOS

003 330
085 300

平 卦 卦 卦
1311583




Cybernews.

4th 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

/Use of Artificial Intelligence as a cause for increased penalty in case of gender-based violence

/Supreme Court penalizes lawyer for petition with AI-generated content and notifies the Federal Council of OAB and OAB-BA to take appropriate measures

/Government creates working group to develop National Cybersecurity Plan

/Access by scammers to bank confidential data results in presumed damages for pain and suffering, according to STJ

/Personal trainer ordered to recover damages for using student's image on Instagram

EDITORIAL

In this edition of the Cybernews Newsletter, we highlight the use of artificial intelligence (AI) as a cause for increased penalty in gender-based violence and the main news on data protection in May 2025.

The Federal Supreme Court penalizes a lawyer for filing a petition with AI-generated content and notifies the Federal Council of the OAB (Brazilian Bar Association) and the OAB from the state of Bahia to take the appropriate measures. The decision found that, in the case in question, AI was used indiscriminately without adequate human review and with the presentation of false information.

In addition, the government has also created a working group to develop the National Cybersecurity Plan, whose goal is to interact with federal government agencies to identify ongoing or planned actions that are compatible with the provisions of the National Cybersecurity Policy (PNCiber) and the National Cybersecurity Strategy (Ciber).

The 3rd Panel of the Superior Court of Justice (STJ in Portuguese) decided that scammers' victims who have their bank confidential data accessed may claim compensation for presumed damages for pain and suffering. The decision was based on a case where an individual paid a fake bank-issued invoice containing confidential information, such as amount and number of installments, which only the bank could know.

Lastly, the 1st Civil Court of Planaltina, in the Federal District, ordered a personal trainer to award damages for pain and suffering to a student for the unauthorized use of his image in a video published on the personal trainer's Instagram account. The decision was based on LGPD (Brazilian General Data Protection Law), and ruled that the processing of the student's data, such as the disclosure of his image, should be based on his "free, informed and unequivocal" consent.

GENERAL NEWS

Use of Artificial Intelligence as a cause for increased penalty in case of gender-based violence

The enactment of Law No. 15,123/2025 represents a significant advance in the fight against psychological violence against women, especially in the digital environment, in which gender crimes have grown exponentially. The law establishes grounds for increasing the penalty for the crime of psychological violence against women, when “committed through the use of artificial intelligence or any other technological resource that alters the victim’s image or sound,” according to a new sole paragraph of article 147-B of the Penal Code.

Psychological violence and the new law

The vulnerability of certain social groups, especially women and young people, is evident and growing in the digital space. Gender-based violence in this environment includes practices such as revenge porn, spreading of fake news, creation of fake profiles on social media, deep fakes, and image manipulation. This social problem is impacted by the new law text in a punitive and preventive manner, as it reinforces the need for changes in society regarding such conducts.

Article 147-B of the Penal Code defines psychological violence as actions that cause emotional damage to women and that harm and disturb their full development or that aim to degrade or control their actions, behaviors, beliefs and decisions, which happens through threat, embarrassment, humiliation, manipulation, isolation, blackmail, mockery, limitation of the freedom of movement or any other means that causes damage to their psychological health and self-determination. With the new law, in situations where such crime is committed through the use of AI or another technological resource that modifies the victim’s image or sound, the penalty is increased by half.

Digital gender-based violence and legislative advances

Data from SaferNet revealed that Portuguese is the second language with the most reports of violence and discrimination against women on online platforms. This statistic underscores the urgency of an adequate legislative response to this serious social problem. The introduction of the cause for increased penalty by Law No.

15,123/2025 is an advance and an example of this.

Over the last decade, there has been a considerable increase in crimes committed in the digital environment, which has been the subject of legislative proposals to curb crimes committed in this space. Likewise, the Penal Code already contains provisions that criminalize the invasion of electronic devices, the unauthorized disclosure of intimate images and even cyber-violence, such as Law No. 12,737/2012 – popularly known as “Carolina Dieckmann Law” – which criminalizes the invasion of a computer device by means of a breach in order to obtain, tamper with, or destroy data or information without authorization.

Law No. 15,123/2025 brings in the first criminal provision specifically related to AI and demonstrates, on the one hand, the current lack of specific mechanisms to combat gender-based violence in these environments and, on the other hand, the attention given to the issue by lawmakers and authorities from various sectors of society. More bills, guidelines and other measures are expected to be published in order to establish greater protection of human rights, encourage diversity and inclusion projects and curb discriminatory practices.

According to the Regulatory Agenda for the 2025-2026 biennium, published by the National Data Protection Authority (ANPD in Portuguese),

the regulation of AI continues to be an agency’s priority for this and the coming years. ANPD has emphasized the relevance of its work in this field, especially considering that technology is intrinsically related to personal data protection.

In addition, Bill No. 2,338/2023, which aims to regulate AI in Brazil, had its text approved by the Senate and is awaiting review by the House of Representatives, which probably will not take place before November of this year. Several topics are still under discussion, such as risk classification, copyright, personal data protection, among others. The Bill prohibits systems considered to be of excessively high risk, especially those that could compromise the protection of fundamental rights, such as in the fight against gender-based violence.

The text also prohibits the use of systems that aim to produce and disseminate material that represents sexual abuse or exploitation of children and adolescents, regardless of its purpose, in order to protect the health, safety, mental and psychological integrity of this group. According to the text of the amendment that included this topic, in 2023, the US National Center for Missing & Exploited Children (NCMEC) received 4700 complaints related to this type of image, which demonstrates the urgency of the matter.

Supreme Court penalizes lawyer for petition with AI-generated content and notifies the Federal Council of OAB and OAB-BA to take appropriate measures

In the judgment of Complaint 78,890, on May 12, 2025, the Supreme Court of Justice (STF in Portuguese), by means of Justice-Rapporteur Cristiano Zanin, denied the complaint because it considered it manifestly unreasonable.

The appeal sought to preserve the jurisdiction of STF and guarantee the authority of its binding jurisprudence – application of Binding Precedents No. 6 and No. 10. However, after a detailed analysis of the appeal, the STF understood that the complainant tried to mislead the Court by citing non-existent or irrelevant decisions to the case and that Binding Precedent No. 6 was cited with false content that was discrepant with the summary. It concluded that the use of false information and the possible use of an AI tool in the preparation of the complaint, without adequate review, represented procedural bad faith.

In this scenario, bad faith was acknowledged, and the claimant was ordered to pay double the initial costs, and the Court ordered the issuance of an official letter to the Federal Council of OAB (Brazilian Bar Association) and to OAB from the state of Bahia, to investigate possible violations of the Statute Governing the Practice of Law.

The decision highlights the importance of technical rigor in preparing court petitions and reinforces that a constitutional complaint cannot be used as a substitute for appropriate resources or lawsuits. In addition, it considers the way in which AI was used in this case to be reckless, highlighting that the draft had the watermark of the tool used, and emphasizes the responsibility of lawyers while using technological tools, to avoid procedural errors and bad faith.



Government creates working group to develop National Cybersecurity Plan

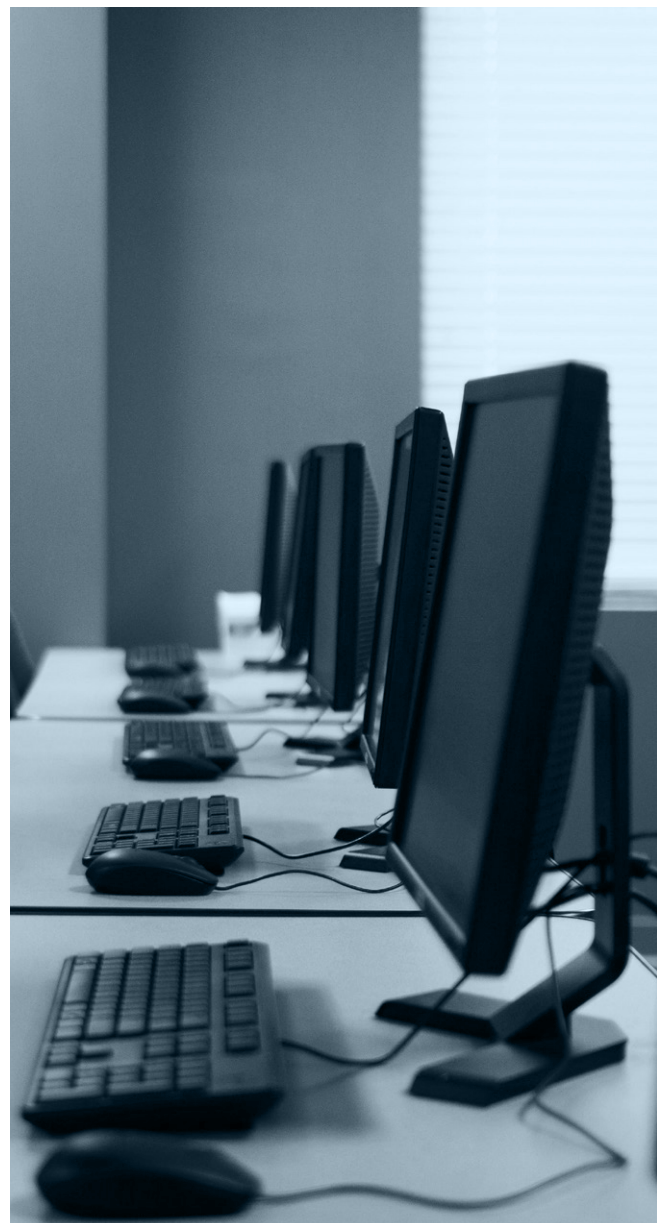
The National Cybersecurity Committee (CNCiber) will create a thematic working group to develop the National Cybersecurity Plan (P-Ciber). The thematic working group will last up to four months, according to a resolution published on May 27, 2025, in the Federal Register (DOU in Portuguese).

In developing P-Ciber, the thematic working group must apply the following guidelines: interact with federal government agencies to identify ongoing or planned actions that are compatible with the provisions of the National Cybersecurity Policy (PNCiber) and the National Cybersecurity Strategy (Ciber); and divide the proposed actions into two groups: short-term actions (2025-2027); and b) medium-term actions (2028-2031).

The thematic working group, which will be coordinated by the Institutional Security Office of the Brazilian Presidency, will include representatives from the government, the business sector, and civil society. At the end of the activities, the coordinator of the thematic working group will sign and submit a final report to the CNCiber for analysis.

The council also published resolutions for the creation of other working groups, such as for developing a guide for the creation and operation of Information Sharing and Analysis Centers; for developing a Guide on Minimum

Cybersecurity Requirements for providers and operators of Essential Services and Critical Infrastructure (SEICs); and for identifying or developing educational materials on cybersecurity and strategies for disseminating these materials.



Access by scammers to bank confidential data results in presumed damages for pain and suffering, according to STJ

In the judgment of Special Appeal No. 2.187.854, the 3rd Panel of the Superior Court of Justice (STJ) decided that scammers' victims whose bank confidential data has been accessed are entitled to compensation for presumed damages for pain and suffering.

The case analyzed involved a victim who paid a fake bank-issued invoice, unaware of the scam, as the criminals presented information that was the bank's responsibility to safeguard and that the victim had not provided.

São Paulo Court of Justice (TJSP in Portuguese) had ordered the bank to reimburse the losses incurred but dismissed the award of damages for pain and suffering on the grounds that the account holder should prove them, such proving that she has become blacklisted for credit or has had her vehicle seized. However, at STJ, although the

Court's precedents demonstrate that bank fraud alone does not constitute pain and suffering, it was determined that the presence of pain and suffering applies in cases involving the leakage of confidential personal data.

According to the court decision, *'the acknowledgment of pain and suffering arises from the evident feeling of insecurity experienced by the party upon realizing that their data has been improperly made available to third parties, facilitating the practice of illicit acts or fraudulent contracts by potential third parties acting in bad faith.'*

Justice Nancy Andrighi, rapporteur of the appeal, concluded that the need to prove actual damage would be unnecessary to assess pain and suffering, as this can be assumed given that there was access to the victim's confidential data.



Personal trainer ordered to recover damages for using student's image on Instagram

The 1st Civil Court of Planaltina/DF ordered a personal trainer to pay R\$600 as damages for the pain and suffering of a student, due to the improper use of his image in a video published on the personal trainer's Instagram account. Even though the student only appeared for three seconds, his image was published without his consent.

During the proceedings, the student reported to be surprised and embarrassed at the content. The personal trainer claimed to have obtained generic consent under the student's contract with the gym, but the judge pointed out that such contract did not authorize the use of his image for the specific trainer.

The judge highlighted that the Constitution guarantees the inviolability of one's image and that the Civil Code requires express consent for public use of such image. She also pointed out that Brazilian General Data Protection Law (LGPD) requires "free, informed and unequivocal" consent for personal data processing. The judge considered the use of the student's image for the defendant's personal promotion as an unlawful action, ordering the personal trainer to recover damages for pain and suffering, in an amount that respects the seriousness of the violation without generating undue enrichment for the student.





Partners responsible for the newsletter

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