




TozziniFreire.

Cybernews

5th 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

Facial recognition and biometric data:
risks and responses from ANPD

Regional Labor Court of the 7th Region
Imposes Fine for Malicious Prosecution
and Refers Case to OAB Due to
Suspected Use of AI

Santa Catarina State Court Denies
Request from Party Who Used AI-Edited
Video as Evidence

STJ Understands that Platform that
Prepares Complaints through AI Should
Continue to Operate

Bitcoin Company Liable for Damages
Caused by Fraud in Transaction

INTRODUÇÃO

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

Check out our opinion on facial recognition and biometric data related to the risks and responses from the National Data Protection Authority (ANPD in Portuguese).

Furthermore, we bring in the decision of the Regional Labor Court of the 7th Region (TRT7), which did not hear an ordinary appeal due to the absence of dialectics and the presentation of non-existent or altered case law due to the suspicion of using artificial intelligence (AI) tools. A fine was imposed for malicious prosecution and it was determined that an official letter was sent to the OAB (Brazilian Bar Association) to investigate a possible disciplinary violation.

Moreover, an appellate judge's decision denied a request in a lawsuit based on an AI-edited video submitted as evidence in a civil-service examination.

The Superior Court of Justice (STJ in Portuguese) has decided to maintain the operation of "Resolve Juizado" platform, which prepares complaints with the assistance of artificial intelligence for BLR 19/90.

Lastly, the 4th Panel of STJ decided that a platform for digital investments in cryptocurrencies should compensate a user who was a victim of fraud, under the understanding that financial institutions are strictly liable for damages caused by internal fortuitous events related to fraud committed by third parties in banking operations.

GENERAL NEWS

Facial recognition and biometric data: risks and responses from ANPD

The use of facial recognition tools has become increasingly common in everyday Brazilian life. It is now typical to find these technologies not only in mobile device unlock features and access control to buildings but also in financial authentication systems, soccer stadiums, and urban surveillance programs.

However, this advancement is accompanied by growing concern: the handling of biometric data, which is classified as sensitive personal data under the General Data Protection Law (LGPD in Portuguese). Due to its unique, immutable, and highly identifiable nature, data such as facial biometrics, fingerprints, voice, and iris require a high level of care and protection. Improper use of these data can have significant impacts on their owners.

In this context, the National Data Protection Authority (ANPD) has been increasingly active, aiming to guide the market and establish legal and technical safeguards for the use of biometric technologies.

In 2024, ANPD published a preliminary study on “Biometrics and Facial Recognition.”

Among the highlighted points, the authority warned about the use of technologies in sensitive contexts, such as public safety, schools, and the consumer market. Furthermore, the need for transparency was emphasized, with clear statutory bases and appropriate use of consent. The document also pointed out the risks of algorithmic biases, which can reproduce racial, social, or economic discrimination, as well as the issue of uninformed collection, which prevents data subjects from exercising their rights and compromises the legal effect of data processing.

Earlier this year, this position took a more concrete form with ANPD’s decision regarding the case of Tools for Humanity, company responsible for the World ID project. The authority ordered the suspension of payment and reward offers in exchange for the collection of biometric data. According to the authority, this type of incentive compromises the freedom of choice of data subjects and invalidates consent, especially in contexts involving vulnerable populations. ANPD also required the company to provide clear

information about the data controller in Brazil, reinforcing its commitment to effectively holding data processors accountable.

More recently, in June 2025, ANPD took another important step by launching a Call for Contributions on “Processing Sensitive Personal Data – Biometric Data.” The inquiry, open to the public until early July, seeks to engage civil society, experts, and the private sector to support future regulation.

The inquiry is organized into thematic blocks addressing fundamental issues such as technical definitions, legal hypotheses for data processing, governance, information security measures, protection of vulnerable groups, and impacts of emerging technologies. With this new step, ANPD aims to ensure that regulation keeps pace with the sophistication of potential uses of this type of data, without compromising the fundamental rights of data subjects.

In this scenario, it is crucial for companies and institutions that handle biometric data, directly or indirectly, to be attentive to the expectations already established by ANPD. Even before the publication of specific regulations, it is possible to identify guidelines that should inform the development and purchase of solutions involving facial recognition or other biometric systems.

Among other aspects, it is important that processing be based on a valid statutory basis, with legitimate, proportional purposes clearly communicated to data subjects. Additionally,

preparing Data Protection Impact Assessments (DPIAs) is recommended due to the processing of biometric data, especially in contexts with higher potential risk. This way, ANPD emphasizes that the collection of biometric data must be transparent, and data subjects should have the necessary tools to understand how their data is being processed, for how long, and for what purpose.

It is worth noting that information security has become a central point in this discussion. Biometric data requires the adoption of higher protection standards to ensure that risks are continuously monitored.

Although the topic is in the process of regulatory consolidation in Brazil, the recent actions of ANPD already provide a robust set of guidelines that organizations can implement immediately. The adoption of biometric technologies, if conducted responsibly and based on a thorough risk assessment, can bring significant gains in security and efficiency. Conversely, indiscriminate use, without appropriate legal and technical safeguards, can result in significant exposures from both regulatory and reputational standpoints. In this context, there is a need to align technological innovation with data governance, ensuring respect for the rights of data subjects and compliance with LGPD from the moment solutions are conceived.

Regional Labor Court of the 7th Region Imposes Fine for Malicious Prosecution and Refers Case to OAB Due to Suspected Use of AI

The 3rd Panel of the Regional Labor Court (TRT in Portuguese) of the 7th Region has unanimously decided not to hear the ordinary appeal in a labor case due to the presentation of tampered case law, with indications of the use of artificial intelligence (AI) tools.

During the review, the TRT identified that the claimant's arguments were generic and did not question the grounds of the decision. Furthermore, the claimant's attorney presented non-existent or altered case law, aiming to mislead the Court.

As a result of the seriousness of this conduct, a fine of 2% on the updated value of the case was imposed, and an official notice was sent to the Brazilian Bar Association (OAB)

– Ceará Section, to investigate any disciplinary violation possibly committed by the attorney.

This decision underscores the importance of ethics and good faith in the practice of law. Appellate Judge Carlos Rebonatto emphasized that tampering case law undermines the integrity of the judicial system and severely violates fundamental ethical principles of the profession.

This case sets a significant precedent in defending transparency and responsibility within the legal sphere, highlighting the crucial role of the attorney in the administration of justice and the conscious use of AI tools as support for legal practice.



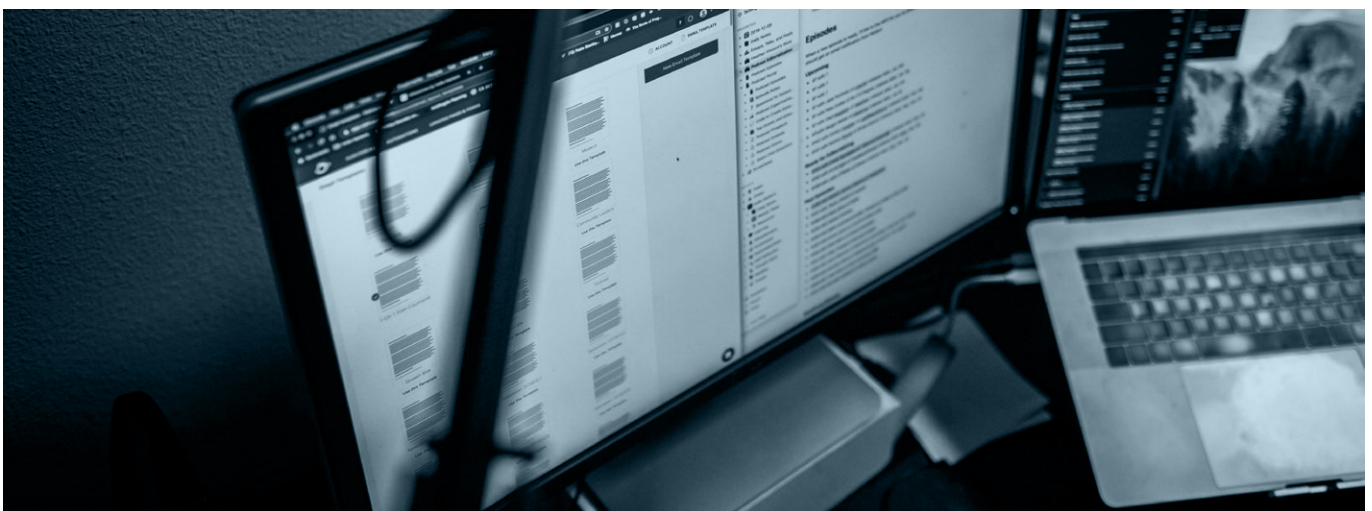
Santa Catarina State Court Denies Request from Party Who Used AI-Edited Video as Evidence

Appellate judge Alexandre Morais da Rosa of Santa Catarina State Court of Justice (TJSC) rejected a request for provisional remedy from a candidate in the Military Police entrance exam, who claimed she was unjustly disqualified in the running test. To prove that she met the minimum time requirement, she submitted a video edited with a digital stopwatch generated by ChatGPT. The judge deemed the material insufficient to validate her claim, as it did not meet the minimum technical requirements to be accepted as expert evidence.

The candidate argued that the manual assessment by the examining board could contain human errors, justifying the video editing. However, the appellate judge stated that the video was not authenticated by a specialized technical report and lacked elements required by technical standards, such as cryptographic hash, digital

certification, software logs, or chain of custody. He emphasized that the insertion of markings in videos using AI must comply with technical standards outlined in regulations such as those from the Brazilian Technical Standards Association (ABNT) ISO/IEC 27.001, 42.001/2024, and NBR 10.520/2023, which address information security, AI management, and source documentation. Thus, the production of private evidence requires adherence to these technical guidelines to ensure forensic and judicial traceability.

The appellate judge also noted the 16-month delay between the disqualification and the lawsuit, which undermined the urgency of the request. The decision does not imply a final rejection but rather the infeasibility of granting an injunction based on evidence not submitted to adversarial testing and lacking technical support, and recommended expert examination as the case is handled.



STJ Understands that Platform that Prepares Complaints through AI Should Continue to Operate

The chief judge of the Superior Court of Justice (STJ), justice Herman Benjamin, has decided to maintain the operation of “Resolve Juizado” platform, which prepares complaints with the assistance of AI for BLR 19,90. OAB-RJ had requested the service to be suspended, arguing that it commercializes the legal profession and improperly attracts clients, but the judge disagreed, stating that the use of technology enhances access to justice.

In his analysis, the justice emphasized that the use of AI in preparing petitions does not violate the legislation, as the tool aims to assist citizens in formalizing their claims in Special Courts, where the presence of a lawyer is not

mandatory. He stressed that the previous decision of the Regional Federal Appellate Court (TRF in Portuguese) of the 2nd Region, which allowed the service to continue, was correct, as there was no concrete evidence of the irregularity alleged by OAB-RJ.

As a result, OAB-RJ announced that it plans to appeal the decision. The controversy began after a public-interest civil action was filed by OAB-RJ against the platform. The trial court ruled the suspension of the platform activities, but the TRF overturned this decision, comparing the platform’s operation to services in other areas that do not represent illegal practice of the profession.



Bitcoin Company Liable for Damages Caused by Fraud in Transaction

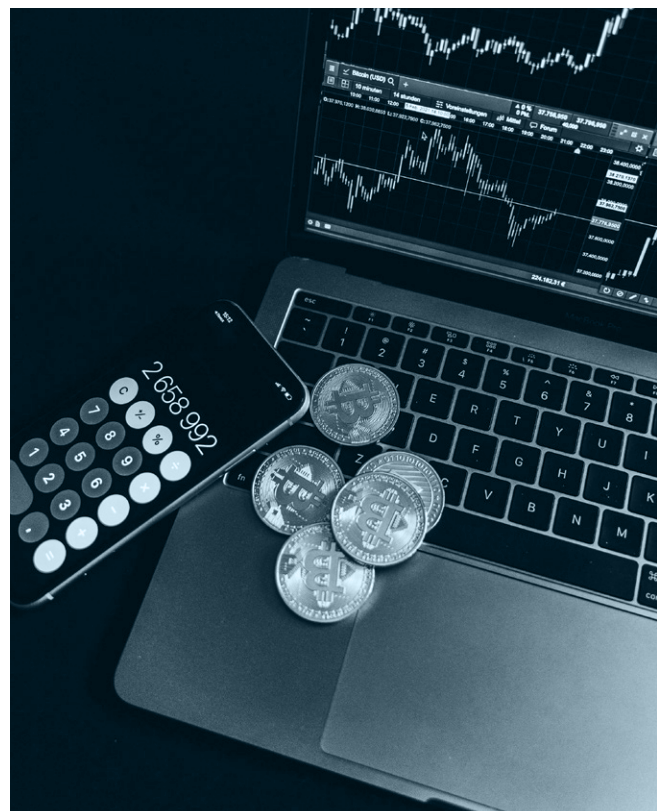
The 4th Panel of the Superior Court of Justice (STJ) ordered a digital cryptocurrency investment platform to compensate a user who was a victim of fraud, ruling that financial institutions, including those trading Bitcoin, are strictly liable for damages arising from internal fortuitous events related to fraud committed by third parties in banking transactions.

In this case, the fraud occurred when hackers accessed the company's system during the user's attempt to transfer funds to another brokerage firm. Reporting Justice Isabel Gallotti understood that the digital investment platform qualifies as a financial institution under Article 17 of Law 4,595/1964, which defines financial institutions as those whose primary or ancillary activity is the custody of third-party assets.

Additionally, there was no evidence that users provided personal information to scammers. However, the court identified a failure in service provision due to the lack of security tools that are adequate to combat cyberattacks, which has led to the platform's liability.

The panel has unanimously upheld the reporting justice's position.

This decision may set a precedent in similar cases, holding cryptocurrency platforms accountable for failing to implement robust security measures to protect users against fraud. Therefore, it is crucial for companies operating in this sector to conduct regular security audits, invest in advanced cybersecurity technologies, and ensure compliance with relevant financial regulations. By proactively addressing these risks, they can mitigate their liability and enhance user trust in their services.





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