TozziniFreire.
ADVOGADOS

Cybernews.

6th Edition | 2024

This newsletter is an informative
of the area of **Cybersecurity & Data Privacy**
of TozziniFreire Advogados.

INDEX

Click on the news and browse the document

EDITORIAL

In this edition of CyberNews, we highlight the main news that permeated the digital and data protection landscape in May 2024.

More than 1,700 people were arrested in Brazil due to the use of facial recognition, even without specific regulations. Bahia leads the way with 1,547 arrests, followed by Rio de Janeiro and São Paulo, which also reported arrests. Several states are implementing the technology, but there are concerns about accuracy and fairness.

Meanwhile, the Central Bank reported PIX key data leaks involving Iugu and Pagcerto, affecting 22,046 keys. The data exposed are registration data, and investigative measures are being adopted.

Ticketmaster confirmed that 560 million customers' data have been leaked. Live Nation is investigating the incident, while Procon-SP (Consumer Protection Office) has notified the company to clarify the impact on Brazilian customers. The Brazilian National Data Protection Authority (ANPD) may demand additional explanations. In the Judiciary, the Superior Labor Court (TST) authorized Banco Santander to use geolocation evidence to prove a bank employee's working hours. The measure was considered appropriate and proportional, without violating privacy.

GENERAL NEWS

Without specific regulations, Brazilian federal states use facial recognition to arrest people

A survey conducted by electronic magazine Consultor Jurídico revealed that more than 1,700 people have been arrested in Brazil due to the use of facial recognition, even without specific regulations. Bahia leads the way, with 1,547 arrests since 2019, followed by other states that use the technology, but do not disclose detailed figures.

São Paulo reported 52 arrests of people wanted by the justice system and other arrests related to court measures and the use of false documents. In Rio de Janeiro, more than 130 people have been arrested since the implementation last New Year's Eve. Roraima detained 15 people at events such as June festivals and agricultural fairs, while Sergipe made eight arrests, despite two cases of mistaken arrests.

Other states, such as Acre, Maranhão and Pará, admitted to using facial recognition, but did not specify the number of arrests. In Minas Gerais, tests at Carnival were well evaluated, but with no arrests.

Several states, including Tocantins, Espírito Santo, Mato Grosso and Goiás, are in the process of implementing the technology. However, Santa Catarina, Paraná, Mato Grosso do Sul, Piauí, Rio Grande do Norte and the Federal District do not use facial recognition. Paraíba, Pernambuco, Amazonas and Amapá did not answer the questions.

Rio Grande do Sul did not provide information due to the environmental tragedy caused by climate change. The lack of data on technological errors and the impact on black and brown people raise concerns about the accuracy and fairness of the use of biometrics.

Central Bank reports PIX key data leak

The Central Bank has released a note informing about security incidents that resulted in the leak of personal data linked to PIX keys, under the responsibility of payment institutions Iugu and Pagcerto. The incidents occurred due to specific failures in the systems of these companies, affecting 19,849 PIX keys from Iugu and 2,197 from Pagcerto.

The Central Bank clarified that the data exposed are registration data and do not include sensitive information such as passwords, financial transactions or account balances. Those affected will be notified exclusively through the mobile application or online banking system of their institutions, without the use of messaging applications, phone calls, SMS or emails.

The Central Bank also stated that the necessary actions for a detailed investigation have already been initiated and that sanctioning measures will be applied in accordance with current regulations. Despite the low potential impact on users, the monetary authority chose to inform the public given its commitment to transparency.

Ticketmaster confirms data leak of 560 million customers

Ticketmaster has confirmed a data leak that may have exposed 560 million customers. Live Nation, which subsidizes Ticketmaster, informed SEC (US Securities and Exchange Commission) that it has launched an investigation after detecting "unauthorized activity" in a third-party cloud database.

On May 28, the hacker group ShinyHunters took responsibility for the attack on the BreachForums forum, offering 1.3 terabytes of data for $500 million. Names, addresses, telephone numbers and credit card information were leaked. The FBI seized the forum's domain, known to be one of the largest on the dark web.

Procon-SP has notified the company to clarify whether Brazilian customers have been affected and how many may have been impacted. Ticketmaster must also clarify how data is stored and what measures will be adopted.

The ANPD (National Data Protection Authority) said it has not received a formal notice from Ticketmaster yet but may demand clarification if it identifies relevant risks or damage to those affected.

JUDICIARY

Superior Labor Court authorizes use of geolocation as proof of working hours

By a majority vote, Subsection II Specialized in Individual Disputes (SDI-2) of the Superior Labor Court (TST) overturned an injunction that prevented Banco Santander from using digital geolocation evidence to prove the working hours of a bank employee from Estância Velha, in the state of Rio Grande do Sul (RS). The panel of judges considered the evidence to be adequate, necessary and proportional, without violating the confidentiality guaranteed by the Federal Constitution.

In the labor lawsuit filed in 2019, the bank employee, who had worked for Santander for 33 years, asked for overtime pay. The bank argued that he held a management position and was not subject to working hours control, requesting its geolocation to check if the employee was on the company premises at the times indicated.

Although the bank employee protested, the request was accepted by the 39th Labor Court of Estância Velha. The bank employee appealed to the Regional Labor Court of the 4th Region (TRT4), claiming violation of privacy, but the TRT4 upheld the decision. Santander appealed to TST, where justice Amaury Rodrigues ruled that geolocation was proportional and appropriate.

The justice pointed out that the measure does not involve the content of communications, but only the location. He also mentioned that the Labor Court is trained in the use of technology and that geolocation can be a valid tool for confirming working hours.

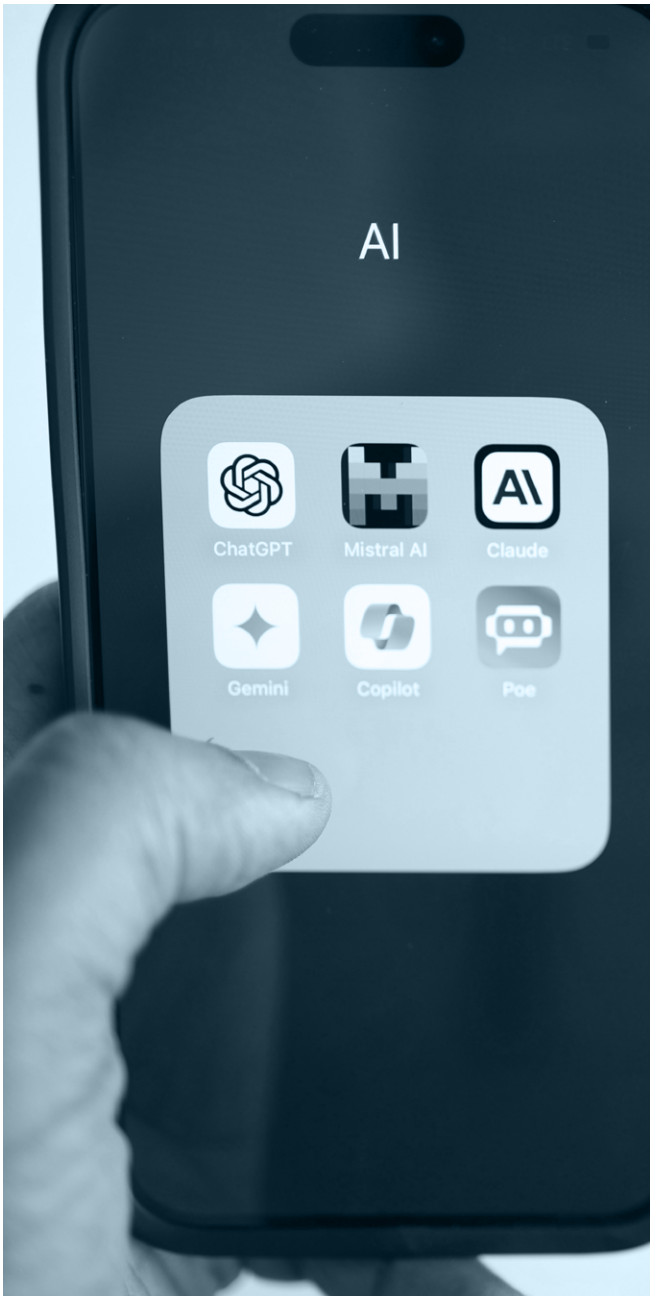
Justices Aloysio Corrêa da Veiga, Dezena da Silva and judge Margareth Rodrigues Costa, who argued that geolocation should be subsidiary evidence, not primary evidence, had a dissenting opinion because they considered the measure invasive.

The Superior Labor Court said that the production of digital evidence is supported by international and Brazilian legislation, such as the General Law on Personal Data Protection (LGPD), the Access to Information Law and the Brazilian Civil Rights Framework for the Internet.

INTERNATIONAL LEGISLATION

New European guidelines on the use and development of generative AI systems

On June 3rd, the European Data Protection Supervisor (EDPS) published guidelines with practical advice regarding the protection of personal data in connection with the use and/or development of generative artificial intelligence (AI) systems for bodies and institutions of the European Union (EU), in accordance with the General Data Protection Regulation (GDPR) (access here).



Notwithstanding the rules and guidelines contained in the EU Artificial Intelligence Act (AI Act), we highlight, below, some of the main guidelines set forth in the guide:

- **Data Protection Officer (DPO)** – the guide emphasizes the DPO's independent advice and assistance role regarding the processing of personal data by generative AI systems. The DPO must understand how the system operates, engage in automated decision-making, and ensure transparency to data subjects. It is also important that the DPO participates in the creation of the Data Protection Impact Assessment (DPIA) and maintains an inventory of the generative AI systems used.

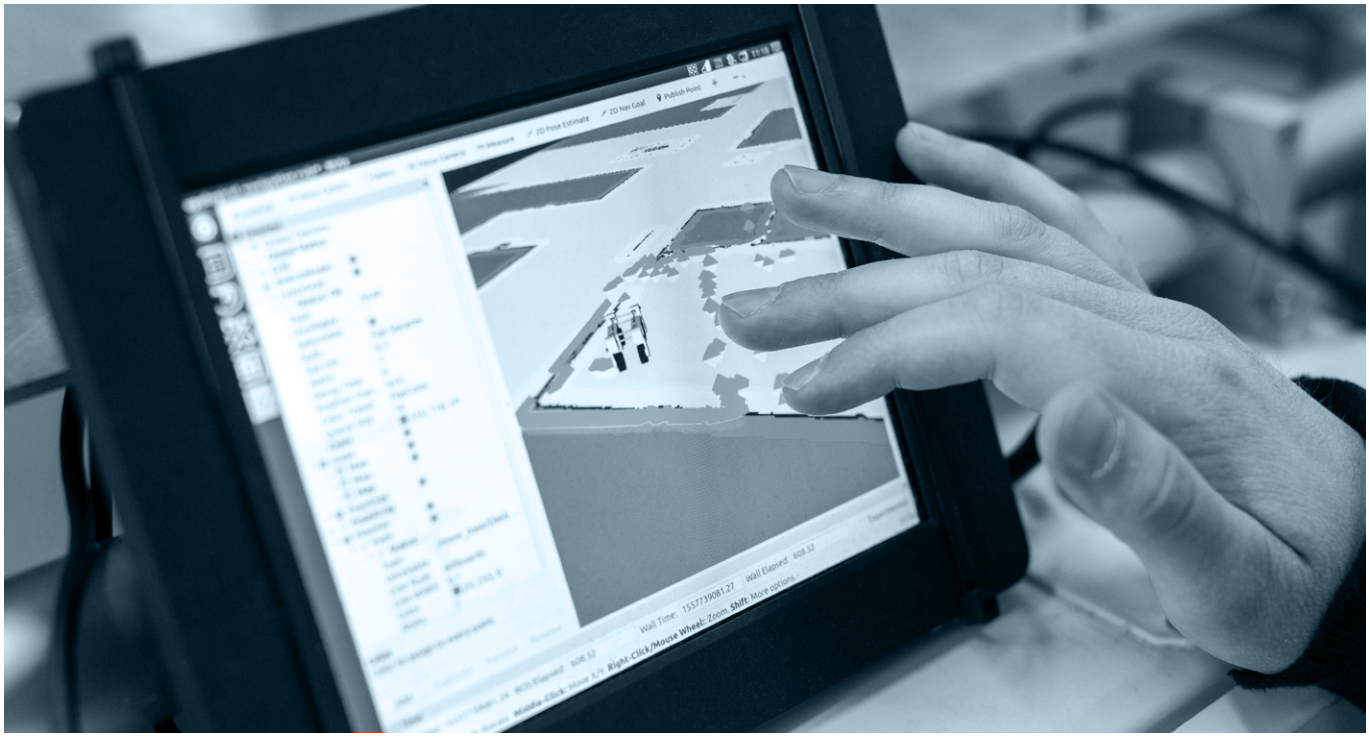
- **Data Protection Impact Report** – the document also recommends the draft of a DPIA before adopting risky operations, which includes new technologies such as generative AI. AI systems' developers must consult the DPO and adopt actions to reduce risks. It is important to review the risks throughout the AI lifecycle, by documenting the decisions taken to ensure transparency and compliance.
- **Lawful bases** – without prejudice to the enforcement of other lawful bases for activities involving generative AI, the EDPS guide addresses two of them more precisely: legitimate interest and consent. Legitimate interest can be used for the collection of data to validate, train, and test the AI system, bearing in mind the situations in which conducting legitimate interest assessment is necessary. Enforcing the lawful basis of consent is delicate and should be done with caution, especially when public data is being processed for AI systems training purposes. Should consent be withdrawn, the data controller must stop the processing if there is no other lawful basis applicable, which may technically impact the AI system.
- **Principle of data minimization** – to ensure the data subjects' privacy, it is essential to control and minimize the use of personal data in generative AI models, ensuring high quality, accurate labels, and clear documentation.
- **Principle of data accuracy** – another recommendation consists of constantly checking and validating the structure and content of the databases used in training AI systems, especially if acquired from third parties, to ensure data accuracy. Monitoring results, adopting contractual clauses to ensure data accuracy, and conducting tests are all important measures to avoid distortions in AI systems.
- **Transparency in AI** – AI systems' developers must provide information on different stages of their development process, as well as the source of data, and other relevant information. When the system interacts with humans, the user should be informed that they are interacting with an AI system.
- **Automated decision-making** – in cases where the generative AI system is used for automated decision-making, the user must be informed about the system's logic, algorithm operation, and databases used, in order to ensure human review.
- **International data transfer** – when the use of the AI system involves international data transfer, compliance with the GDPR lawful bases is mandatory.

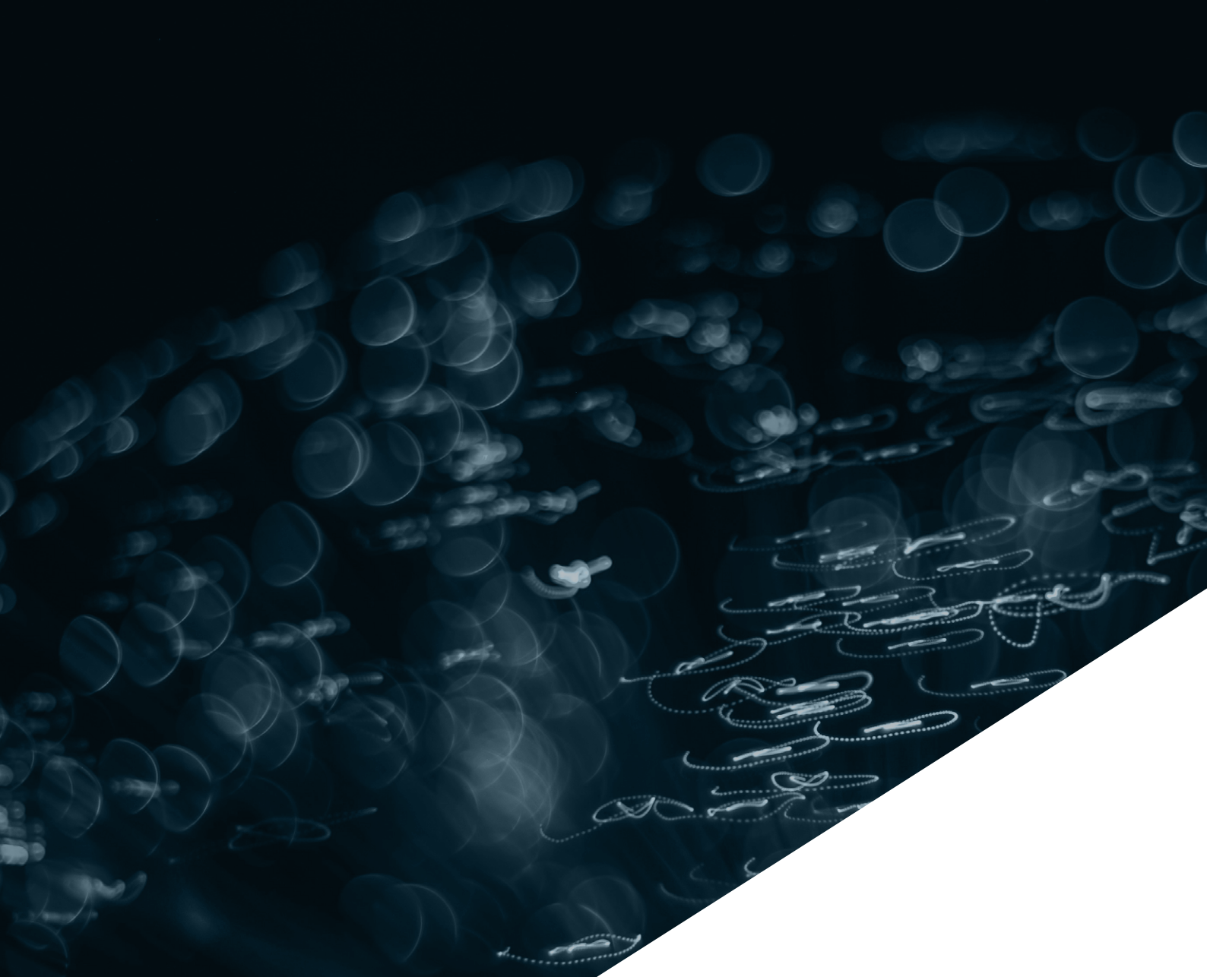
The guidelines issued by the EDPS, in compliance with the GDPR, offer valuable guidance not only for European companies

and institutions, but also for Brazilian companies seeking to anticipate and mitigate risks associated with generative AI systems. By following these guidelines, institutions can address the challenges and identify the benefits arising from the responsible and transparent use of technologies based on AI systems. This alignment with established best practices contributes to an ethical and effective approach to implementing technologies that use AI systems, aligning with global data protection principles.

Looking at the Brazilian reality, the Brazilian Legal Framework for Artificial Intelligence is still being discussed at the National Congress. The voting was expected to take place on June 18, 2024, but it was postponed due to the presentation of a new version of the Bill by the Internal Temporary Commission on Artificial Intelligence in Brazil. The proposed changes include the indication of the National Data Protection Authority (ANPD) as the entity responsible for coordinating the National System for Regulation and Governance of Artificial Intelligence (SIA). As a result of the presentation of this new wording, the vote on the AI Legal Framework was postponed and will take place after five public hearings on the subject in the committee.

As a definition on the Bill aiming to regulate the use of AI systems in Brazil is awaited, it is worth mentioning the role that the ANPD has been playing regarding this topic. The authority has already published a series of documents analyzing the current Bill, made contributions to the replacement text proposed by the Bill's senator-rapporteur and included in its regulatory agenda for the 2023-2024 biennium the edition of some actions involving this subject.





Partners responsible for the newsletter

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

Contributed to this newsletter:

Beatriz Guthmann Spalding
Carolina Vargas Pêgas Bonfante
Caroline Cristina Malheiros
Igor Baden Powell
Isabella de Freitas Moraes Sampaio Pereira
Julia Parizotto Menzel
Julie Lissa Kagawa
Luciana Pinto de Azevedo
Maria Eugênia Geve de Moraes Lacerda
Mariana Costa Alvarenga
Miguel Lima Carneiro
Steffani da Silva Nepomuceno
Tatiane Robles Martins
Valentina Garcia de Victor