

**Tozzini  
Freire.**

ADVOGADOS

**CYBERNEWS.**

32<sup>nd</sup> Edition | 2023

# Index

## 01

..... 03

..... 05

..... 06

..... 07

..... 08

## 02

..... 09

..... 10

## 03

..... 11

..... 12

## 04

..... 13

## 05

..... 14

## 06

..... 15

# 01

# Brazilian Context.

## **ANPD imposes two new sanctions against government agencies**

---

Continuing its enforcement work, in October ANPD imposed two new sanctions against government agencies in the states of São Paulo and Santa Catarina.

The first decision by the General Inspection Coordination (CGF), published in the Federal Official Journal on October 6, concluded an administrative sanctioning process against the São Paulo State Public Servant Assistance Institute (IAMSPE).

The CGF found that IAMSPE had breached Article 49 of LGPD, due to the lack of security in the storage and processing of personal data of civil servants and their dependents. In addition, the body failed to properly communicate a security incident to data subjects, in breach of art. 48 of LGPD.

As a sanction, the CGF issued two warnings to IAMSPE, one for each infraction. In addition, corrective measures were established to improve the security of data storage systems and ensure clearer communications with data subjects.

The CGF's second decision, published in the Federal Official Journal on October 18, concluded the administrative sanctioning process against the Santa Catarina State Health Department (SES-SC).

The understanding was that SES-SC, just like IAMSPE, infringed art. 49 of LGPD, due to the lack of security in the storage and processing of personal data of the population in Santa Catarina that uses the state public health system, and, consequently, did not properly communicate a security incident to more than 300,000 data subjects, infringing art. 48 of LGPD.

In this sense, due to the failure to submit the Personal Data Protection Impact Report (RIPD) and the other information requested by ANPD, art. 38 of LGPD and art. 5 of ANPD's Supervisory Regulation were violated.

As a sanction, the CGF issued four warnings to SES-SC, one for each infringement. Specifically in relation to the infringement of art. 48 of LGPD, corrective measures were established to keep on the internet a general notice of security incident for a period of 90 days, as well as directly inform the personal data subjects who had their data leaked in the incident.

The government agencies may appeal the decision to ANPD's board of directors within 10 working days of ANPD's notification.



## **ANPD closes administrative sanctioning proceeding against Rio de Janeiro Botanical Garden Research Institute**

---

On October 6, 2023, ANPD (Brazilian Data Protection Authority) closed the Administrative Sanctioning Proceeding filed against Rio de Janeiro Botanical Garden Research Institute, due to indications of infringement of LGPD (Brazilian General Data Protection Law).

The case was filed after ANPD received a complaint that the Rio de Janeiro Botanical Garden had improperly processed the personal data of visitors to the park. Specifically, the complaint alleged that the Botanical Garden had collected personal data from visitors without their consent and had shared this data with third parties without proper authorization.

However, after analyzing the case records, ANPD concluded that there was insufficient evidence to support the allegations. The case was therefore closed as ANPD did not identify any conduct that could constitute violations to LGPD.

ANPD's decision is important, as it demonstrates the Authority's commitment to investigate complaints received and to apply corrective measures only should it find the necessary evidence.

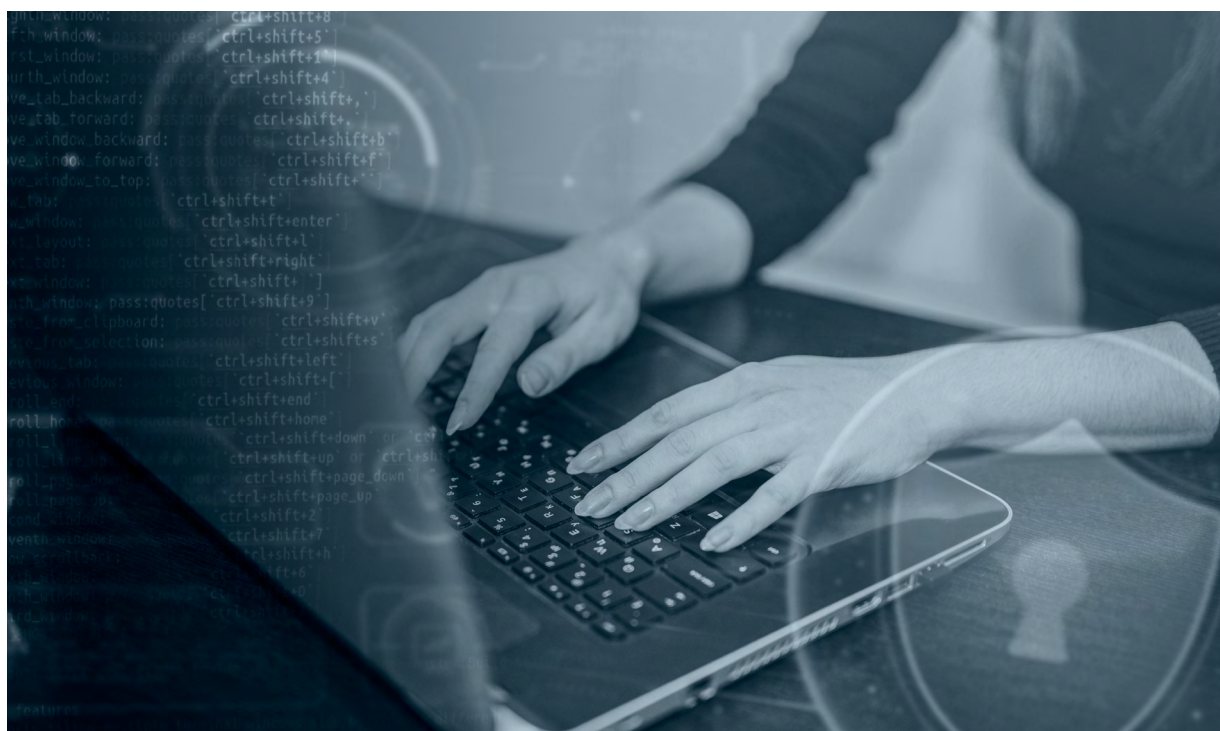
## **ANPD: Regulatory sandbox for AI and personal data protection**

---

ANPD launched a public inquiry on a regulatory sandbox for Artificial Intelligence (AI) and data protection in Brazil.

The regulatory sandbox is an environment controlled and monitored by a regulatory authority for the use of new technologies, such as AI. ANPD's aim is to collect experiences and knowledge for drafting future regulations on AI, based on the following scope: (i) machine learning (ML), i.e., AI processes through which computers learn and improve their performance, from one or more databases, in an automated way and without human intervention; and (ii) generative AI, which is AI systems that create content such as images, music or texts, based on previous patterns/data, in a predictive way.

Contributions can be sent via the [Participa + Brasil Platform](#) until November 1, 2023.





## **Anatel conducts Cybersafe October campaign**

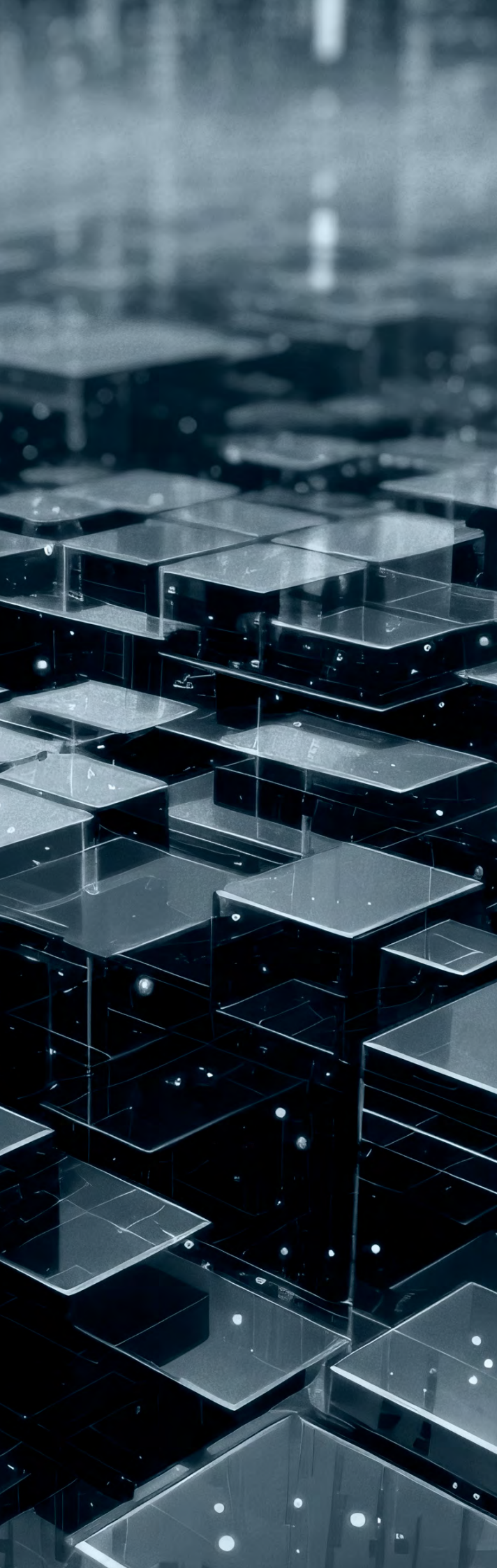
---

As part of the Brazilian Telecommunication Agency's (Anatel) Strategic Plan for 2023-2027, Anatel promoted several actions against cyber threats and to boost the conscious use of the digital environment.

The actions comprise videos, posts, and speeches about the protection of children and teenagers on the internet, in view of the Brazilian Children's Day. The hot topics include frauds in the digital environment and precautions when having your cell phone stolen.

Besides that, the Center of Studies, Response and Processing of Security Incidents in Brazil (CERT.BR) published guides with safety tips.

The materials and guides are available on the links: [CERT.BR](#) e [ANATEL \(in Portuguese\)](#).



## **Blockchain could revolutionize Government activities, but it requires compatibility with the LGPD**

---

During a hearing in open court at the House of Representatives, a representative of ANPD's Board of Directors addressed the use of blockchain as a strategy to improve Government activities.

Blockchain would reduce bureaucracy and prevent corruption or fraud, but its implementation requires caution due to its decentralized data management and the difficulty in identifying, measuring, and fighting any potential incidents or malfunctions.

There was a debate about the topic, whose paper with the pros and cons chart analyzing the use of blockchain by the Government, as well as the importance of innovation as a Constitutional Principle is [available here \(in Portuguese only\)](#).





# Judicial Branch.

## **Caixa, Dataprev and ANPD should pay damages from BRL 15,000 to 4 million to citizens who had their personal data leaked**

---

The Federal Court has ruled that approximately 4 million people will be compensated BRL 15,000 each by Caixa Econômica Federal, Dataprev and ANPD, due to a massive data leak that occurred in the second half of 2022, related to the Auxílio Brasil program. The decision can still be appealed.

The public interest civil action was originally filed by the Brazilian Institute for the Defense of Personal Data Protection, Compliance and Information Security, with the support of the Federal Prosecution Office, on the grounds that the illegally leaked personal data ended up in the hands of banking correspondents, who used the information to offer loans and other financial products.

In addition to individual damages, the judgment established compensation of BRL 40 million for collective pain and suffering, to be allocated to the Fund for the Defense of Diffuse Rights. The defendants were also obliged to formally notify data subjects of the security incident, the measures adopted to mitigate the damage and the plans to resolve any possible risks.

The decision by federal judge Marco Aurelio de Mello Castrianni also imposes several obligations on the parties involved, including the disclosure of internet connection records, access to records by affected data subjects and the preparation of independent reports on the impact on personal data protection. In addition, it stipulates fines in the event of non-compliance with the measures determined and the registration of the action in the National Council of Justice (CNJ)'s National Register of Class Action Information.

## **Brazil's National Council of Justice launched a public tool to universalize access to information regarding legal cases**

---

A new API launched by the National Council of Justice (CNJ) allows anyone to access relevant information related to legal cases in Brazil, such as lawsuit number, the State or Federal Court responsible, current status and most relevant case developments.

The API allows the centralized storage on data of multiple lawsuits, encompassing digital and physical cases, except for those closed to the public.

According to the National Council of Justice, LGPD's provisions are respected, and no confidential information will be disclosed.

The National Council of Justice aims to provide more transparency and simplify access to metadata for the general public, Judiciary branch members, legal practitioners and researchers.



# 03

## Authorities.

### **Agreement between CBF and the Ministries of Sport and Justice approves use of facial recognition in soccer stadiums**

---

On September 20, the Ministries of Sport and Justice signed a cooperation agreement with CBF (Brazilian Football Confederation) to implement the “Safe Stadium Project,” which aims to improve security in soccer stadiums throughout Brazil. The project includes the use of facial recognition, information sharing with the Ministry of Justice, identification of people with outstanding arrest warrants, among other measures. Participation by clubs is optional.

At the same time, at the municipal level, the São Paulo Public Prosecutor’s Office (MPSP) has issued an injunction to suspend the contract with the Smart City Consortium, responsible for the Smart Sampa program, which involves monitoring and facial recognition in the management of city hall. The lawsuit, filed by the PSOL (Socialism and Liberty party) Feminist Movement, alleges risks of racism in the use of the technology and violation of the Brazilian General Data Protection Law. The prosecutor recommended the suspension of the contract, citing concerns about potential unjust arrests of black people.

Both cases highlight the ongoing debate about the use of facial recognition in Brazil, with concerns related to security, privacy, and possible discriminatory consequences. While the project in soccer stadiums aims to improve the safety of fans, the lawsuit in São Paulo questions the ethics and legality of using the technology in an urban context, especially in relation to the processing of personal data and issues of racial discrimination.

## São Paulo City Hall creates data protection coordination

---

The Office of the Controller General of the City of São Paulo has established a new data protection coordination to bring municipal bodies into line with the Brazilian General Data Protection Law (LGPD). The measure seeks to ensure uniformity in the enforcement of LGPD in all municipal departments, regional city hall offices, and companies. The controller general, Daniel Falcão, stresses the importance of respecting LGPD, as the city's digital services continue to expand.

The new coordination has provided a manual with practical guidelines to guide municipal bodies on which data to disclose and which to keep confidential. One of the challenges is to balance LGPD with the Access to Information Act (LAI) so as not to jeopardize transparency upon disclosing information.

In addition, data protection is especially critical in sensitive projects such as Smart Sampa, which involves the use of cameras with facial recognition in public spaces in the city of Sao Paulo. The implementation of this program is being closely monitored to ensure its compliance with regulations.



# 021 Normative Developments.

## Bill to enforce the disclosure of security incidents involving personal data in media channels

---

Since August 2023, the House of Deputies has been analyzing Bill No. 1,876/2023, proposed by representative Marcos Tavares, which aims to enforce the disclosure of security incidents that may pose a risk to data subjects. This includes disclosure in widely known media channels, as well as on the websites and profiles of data processing agents, in addition to notifying ANPD.

The Bill intends to include this measure in LGPD and to provide greater transparency in such cases, as well as allowing data subjects and ANPD to adopt measures to repair the damage and to prevent similar incidents.





# Court Decisions.

## **Rosa Weber votes against disclosure of user's access and connection records on platforms**

---

On September 22, the chief judge of the Federal Supreme Court (STF), justice Rosa Weber, voted against access by the Rio de Janeiro Public Prosecutor's Office (MPRJ) to access and connection records of unidentified users. She considered the "reverse search" procedure to obtain information on people who have searched for certain terms and periods of time (reverse search history) to be invalid. This judgment will have significant implications for the definition of limits to breaching the confidentiality of users' search history on platforms.

The case is related to the investigation into the murder of Marielle Franco and Anderson Gomes in 2018 and reached the STF after the Superior Court of Justice (STJ) ordered Google to provide the MPRJ with data of an unidentified group of people who searched for Marielle. Google argued that if this decision were validated, it would set precedents for other violations of privacy.

In her vote, the chief judge of the STF highlighted the lack of legal basis for the breach of confidentiality, arguing that the Brazilian Civil Rights Framework for the Internet (MCI) does not allow generic court orders for the provision of connection and access records of users who have searched for specific terms on application providers. She also emphasized the disproportionality of the reverse search, especially in relation to the period of time specified by the MPRJ.

# 06 International Rulings.

## France: penalty imposed for excessive collection of employees' personal data

---

The French Data Protection Authority (CNIL) has imposed a fine of 200,000 euros for the excessive collection of personal data relating to the private lives of employees of airline SAF LOGITICS.






In addition to the excessive collection, CNIL found several breaches of the data protection legislation, including failure to comply with the authority's orders that prohibited the collection of sensitive data and criminal records, as well as failure to cooperate with CNIL during the investigation.



Newsletter content produced by TozziniFreire's  
Cybersecurity & Data Privacy practice.

**PARTNERS RESPONSIBLE  
FOR THE CONTENT:**

Marcela Waksman Ejnisman

-  Patrícia Helena Marta Martins
-  Carla do Couto Hellu Battilana
-  Bruna Borghi Tomé
-  Luiza Sato
-  Sofia Kilmar

For further information, please visit:

[tozzinifreire.com.br](https://tozzinifreire.com.br)

**Tozzini  
Freire.**  
ADVOGADOS