

Tozzini Freire.

ADVOGADOS

CYBERNEWS.

31st Edition | 2023





Index

01

..... 03

..... 04

02

..... 05

03

..... 07

..... 08

04

..... 09

..... 10

05

..... 11

..... 12

..... 13

06

..... 14

..... 15



Brazilian Context.

ANPD's latest activities

Between August and September, the Brazilian Data Protection Authority (ANPD) has been very active and published some institutional documents, whose key points are described below:

- **Monitoring Cycle Report (RCM)** – which illustrates the assessment of ANPD's inspection activities in 2022 and its main results: for instance, receipt of 1,045 requests, including complaints for breaches of the Brazilian Data Protection Law (LGPD), and petitions from data subjects. Sectors with the highest number of requests were digital platforms, finance, telecommunications, and data aggregators. Regarding security incident communications, 473 notifications were received, and the majority of cases relate to cyber hijacking caused by security breaches in information systems (ransomware).
- **Social Communication Policy** – which aims at guiding ANPD's strategic social communication actions to promote the empowerment of data subjects.
- **Mid-year Monitoring Report** – which details the development of projects considering the 2023-2024 Regulatory Agenda. According to the report, the following actions are still expected to take place by the end of this year: approval of the Regulation on the Communication of Personal Data Breaches, public inquiry about the Regulation on the Data Protection Officer Role, and publication of further guidelines.



Debate on ANPD's sanctioning activity

In August, a public hearing was held by the Economic Development Commission (CDE, in Portuguese) of the House of Representatives regarding administrative sanctions applied by ANPD resulted from personal data breaches. The purpose of the hearing was to discuss the allocation of fines related to such data breaches, and other possible improvements to the Brazilian LGPD.

At the hearing, the General Supervision Coordinator of ANPD highlighted that the LGPD and ANPD go beyond matters related to data breaches, and that the authority's actions are based on the attitude of the processing agent that is being supervised in a progressive manner - from monitoring, guidance, and repression, whenever necessary.



Judicial Branch.

National Council of Justice begins monitoring cycle for implementation of LGPD resolution

On August 25, the National Council of Justice (CNJ) launched the cycle for monitoring and evaluating the regulatory outcome of Resolution No. 363/2021, which establishes guidelines for adapting to the General Data Protection Law (“LGPD”) in the courts of Brazil. This took place during the 1st National Symposium on LGPD in the Judiciary Branch, promoted by the Court of Justice of Bahia (TJBA), which brought together several institutions, including the Superior Court of Justice (STJ), CNJ, state and federal courts, and the Brazilian Data Protection Authority (ANPD).

Councilor Luiz Fernando Bandeira de Mello, coordinator of the Personal Data Protection Steering Committee (CPGD) and responsible for the processing of personal data at the National Council of Justice, pointed out that the field of data protection is still under development in Brazil, and emphasized that the regulatory evaluation aims to discuss the results and impacts of the regulation based on empirical data.

For him, the resolution plays a crucial role in enforcing the fundamental right to personal data protection. “Our goal is to identify where we are, that is, to map out the regulatory challenges and the preventive and corrective measures needed to address these issues. This evaluation model is designed to guarantee this process,” he points out.

The National Council of Justice will send a questionnaire to collect key information to State Courts, divided into identification, evaluation, and perception. It will also maintain a permanent channel to answer questions while the survey is filled out, recognizing the complexity of the regulatory demands arising from Resolution No. 363.

03

Authorities.

São Paulo Public Prosecutor's Office investigates possible illegality in São Paulo government's submission of student data to advertising companies

The São Paulo Public Prosecutor's Office (MPSP, in Portuguese) has launched an investigation into whether the State Department of Education (SEDUC) violated the General Data Protection Law (LGPD) and violated students' right to privacy by allegedly collecting their personal information during the pandemic and forwarding it to specialized advertising companies.

The complaints were made by the NGO Human Rights Watch (HRW), which reported that the irregularities occurred through the São Paulo Education Media Center (CMSP) and other platforms that provided services to SEDUC. According to HRW, the websites not only monitored students in virtual classrooms, but also during their whole time on the internet, obtaining information about the private lives of children and adolescents.

Based on HRW's research, prosecutor Sandra Lucia Garcia Massud opened an investigation and gave SEDUC 30 days to provide a copy of the documents signed with the platforms, in order to analyze the contracts and check whether data was collected and processed, as well as whether it was disclosed to advertising companies.

The administration of the governor of São Paulo, Tarcísio de Freitas, said that it had not signed any contracts or had any relationship with the platforms mentioned in the complaint. The contracts were signed by previous administrations and were terminated in 2021 and 2022. The Media Center continues to operate, but with a different personal data processing system, limited only to what is necessary to accomplish the educational purpose.

Conar closes case against the advertisement that recreated Elis Regina with AI

The case initiated by the Brazilian Advertising Self-Regulation Council (CONAR) to analyze Volkswagen's campaign was closed by the Ethics Board on August 22, 2023. The campaign, launched on July 4 and created with Artificial Intelligence, was analyzed to determine whether it violated Brazil's Self-Regulatory Advertising Code.

The ethical proceeding initiated by CONAR stems from consumer disagreements over two main aspects: (i) questions on whether a video ad that used hybrid generative Artificial Intelligence to recreate the image of singer Elis Regina, who died in 1982, was made with respect and ethics; and (ii) inquiries about the need to include explicit information in the advertisement regarding the use of this AI tool in its creation.

In an official note, CONAR said that "the board unanimously considered the question of disrespect for the artist's image to be unfounded, since the use of her image was made with the consent of her heirs and observing that Elis appears doing something she did in her life."

Regarding the obligation to disclose the use of the deepfake AI technique, CONAR reported that it evaluated several good practices guidelines that already exist on the subject, "as well as the absence of specific regulations in force." In view of this, the majority of the board members chose to dismiss the complaint.

Besides that, the Council added in a statement that transparency is a fundamental ethical principle and was respected, emphasizing that the case was addressed with fair hearing.

021 Normative Developments.

New guidelines on sending bulk communications are published by the British Information Commissioner's Office

On August 30, the British Information Commissioner's Office (ICO) issued new guidelines advising on the submission of bulk emails, specifically warning organizations about the risks involved in this process. In its guidelines, the ICO outlines recommendations for best practices related to the protection of personal data in such context.

The relevance of using appropriate methods when sending mass communications is emphasized based on recent ICO enforcement actions, which have identified recurring cases of unnecessary data disclosure based on mistakes made when sending email communications. Although there is still no specific guidance from the ANPD on the matter in Brazil, the ICO guidelines are directly aligned with the general warranties outlined in the Brazilian applicable data protection regulations.





Canadian Centre for Cyber Security issues recommendations on mobile app privacy

In August, the Canadian Centre for Cyber Security published recommendations for users, data subjects, and organizations, on personal data protection during the use of mobile applications.

The text provides guidance on data that can be collected by mobile applications, the risks inherent in sharing data with these applications, how users can protect themselves from these applications, among other information. You can read the complete guidelines and recommendations [here](#).



Court Decisions.

São Paulo Court of Justice dismisses order for payment for pain and suffering in data leak case

The 25th Chamber of Private Law of the São Paulo Court of Justice rebutted the presumption of pain and suffering in a data leak case. In short, the Court held that the data was not sensitive and that there was no proof of damage, since no real harm has been caused by the incident.

The case involved an action for damages brought by a consumer, alleging that his data had been misused by swindlers after he had taken out a life insurance policy with the insurer.

The lower courts ordered the insurer to pay R\$10,000, but after the insurer filed an appeal, the court reversed the decision. The judge-rapporteur pointed out that the insurer was not liable for the leak and that there was no connection between the alleged damage and the data incident.

He also stated that the leaked data cannot be considered “sensitive data” according to the definition under Article 5 of the LGPD, therefore ordering the insurer to make any payment is unjustifiable.

Superior Court of Justice restricts Google's provision of data to identify users

The 6th Panel of the Superior Court of Justice (STJ) partially upheld Google Brasil's appeal on the grounds that it is necessary to provide data to the courts in order to help investigate a crime. However, the Court states that the extension of the breach of data confidentiality must be limited to information sufficient to identify users, such as connectivity records and access to applications, ruling out broad and unrestricted access to content such as e-mail and photos.

The case involves a police investigation into a serious crime of robbery that resulted in murder. Initially, the lower court authorized, at the request of the police chief, "the breach of confidentiality of telematic data of users who may have used Google's services within a radius of 500 meters of the geographical coordinates in the period between 6:00 p.m. and 10:00 p.m. on May 22, 2022".

In the judgment of the appeal filed against such order, the judge-rapporteur, justice Laurita Vaz, initially ruled that the objected decision was not written in a generic manner, nor did it violate the right to privacy of users of the services offered by Google. Justice Schietti sided with the judge-rapporteur.

It was following a vote by Justice Sebastião Reis, who dissented on the grounds that Google's provision of information should be limited and that the company should "provide only and exclusively the information necessary to identify the IP", that the judge-rapporteur reconsidered her vote and agreed with the need to limit the set of data to be provided by the company. The other justices, Rogério Schietti and Saldanha Palheiro, also agreed with this last understanding.

In the end, it was noted in the judgment that there is nothing to prevent the request of further information in the future from the ones being investigated, provided this is justified. All the ministers agreed with the observation.

Judge in São José dos Campos decides that financial institution is strictly liable for leak of account holder data

Judge Marcos Alexandre Bronzatto Pagan, of the 2nd Small Civil Claims Court of São José dos Campos (SP), ordered a financial institution to refund the total amount of R\$32,800.00 to an account holder who was the victim of fraud and induced to make bank transfers after having her personal data leaked.

The facts discussed in the lawsuit indicate that the consumer and account holder transferred money via Pix to a scammer who used confidential information obtained from her bank account.

As grounds for the decision, the magistrate judge noted that the evidence presented by the consumer – i.e. proof of transactions, emails exchanged with the financial institution's employee, account statements and records of telephone calls – was sufficient. In addition, the good faith of the consumer, who was already an old account holder and had no previous record of similar events, was presumed.

Based, therefore, on the rules of the Consumer Protection Code and on the premise that the financial institution leaked the account holder's sensitive data due to "a representative or through the bank service channels, that is, when generated by an internal incident," the decision ordered the financial institution to compensate the amounts spent by the consumer due to the fraud, following the recent case law of the São Paulo State Court of Justice.

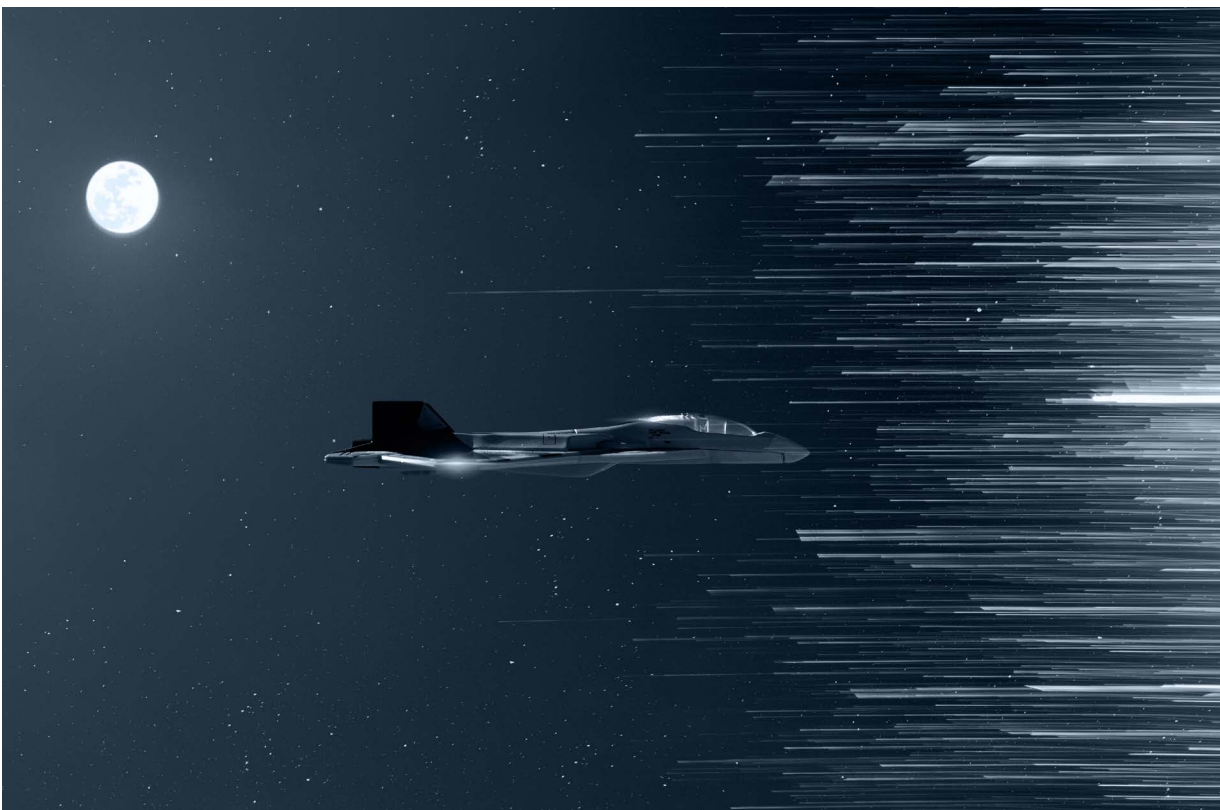
06

International Rulings.

Spain creates Europe's first AI supervisory agency

In late August, Spain's Council of Ministers approved the statute of AESIA – the Spanish Agency for the Supervision of Artificial Intelligence – authorizing its creation, becoming the first European country to have an agency to regulate this subject and anticipating the European Artificial Intelligence Regulation's enactment. AESIA aims to protect citizens, oversee the development of inclusive, sustainable and citizen-centric Artificial Intelligence, and enforce regulations on Artificial Intelligence.

Please see the full ministry statement [here](#).





Update on the approval framework for data protection officer certification bodies in France






In France, some certifying entities, previously approved by the French Data Protection Commission (CNIL), can issue certification to data protection officers (DPOs). This certificate is a voluntary and an optional mechanism that proves that the DPO actually complies with the requirements of having the skills and knowledge on the European Data Protection Regulation (GDPR).

The approval granted by the CNIL to certifying entities is based on an analysis of various requirements, which were updated in August. Among these updates, it is worth noting that, as of now, any DPO seeking such certification must be able to demonstrate their skills on the matter by presenting specific documents – even though the certification fundamentals remain unchanged. In addition to that, certifying entities are no longer required to demonstrate previous experience in the area of people certification as before.

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

**Tozzini
Freire.**
ADVOGADOS