

**TozziniFreire.**  
ADVOGADOS




# Cybernews.

---

4<sup>th</sup> 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 

## 01 | Editorial

---

## 02 | Legislative

---

/Conanda Resolution No. 245/2024, regarding rights of children and adolescents in the digital environment, is approved

## 03 | General News

---

/TozziniFreire Advogados hosted the event “PrivacyRules 2024 Latin American Conference”

/Fiesp holds event encouraging dialogue between the public and private sectors

/Companies face pressure to meet equal pay reporting deadline

/Brazil makes progress in the implementation of “open health”

/Brazilian Federal Police has arrested the suspect in Brazil’s largest data leakage

## 04 | Bills

---

/Bill provides for regulation of personal data monetization

## 05 | Judiciary

---

/The Superior Electoral Court signed new agreements to combat deepfakes and hate speech in municipal elections

# EDITORIAL

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

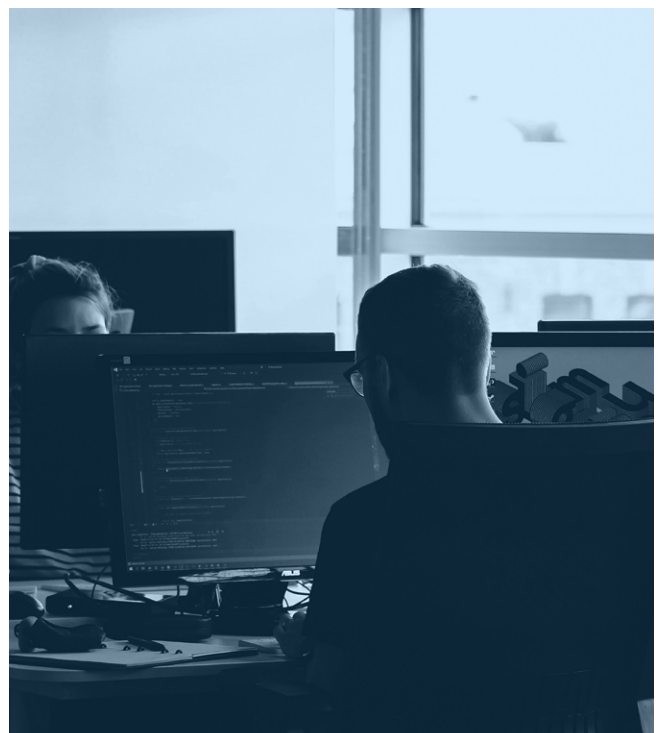
In the last newsletter, we discussed the stronger commitment to the enforcement of LGPD by the Labor Prosecution Office in relation to its position for maintaining the Equal Pay Report, by the City Hall of São Paulo when assuming the Presidency of the Municipal Data Protection Forum, and by the Prosecution Office in the investigations into the use of the citizen's Tax ID by drugstores to offer discounts.

Earlier this month, we pointed out that challenges continue as companies face pressure to meet equal pay reporting deadlines. In a recent decision, the Federal Court of the 6th Region suspended the effects of the injunction that exempted companies with 100 or more employees from disclosing salary transparency reports.

On another front, there was progress in the implementation of "open health" in Brazil, and the Federation of Industries of the State of São Paulo (Fiesp) held an event to discuss the most appropriate ways to respond to cyber incidents. Also, the Federal Police

arrested the suspect of the largest data leakage in Brazil – which occurred in 2021.

Also noteworthy is the performance of the legislative branch, through the National Council for the Rights of Children and Adolescents (Conanda), in the approval of Conanda Resolution No. 245/2024, which provides for the rights of children and adolescents in the digital environment, as well as in the discussion of Complementary Bill No. 234/2023, which intends to establish the Data Empowerment General Law (LGED), which will provide for the Brazilian data monetization ecosystem in Brazil.



# LEGISLATIVE

## **Conanda Resolution No. 245/2024, regarding rights of children and adolescents in the digital environment, is approved**

In April 2024, Brazil's National Council for the Rights of Children and Adolescents (Conanda) approved Resolution No. 245/2024, which provides for the rights of children and adolescents in the digital environment.

In summary, the Resolution highlights the importance of digital technologies in the contemporary scenario, underlining their role in both promoting and jeopardizing the rights of children and adolescents. The term "digital environment" is applied to a wide range of information and communication technologies, including the internet, connected devices, virtual and augmented reality, artificial intelligence, robotics, and other advanced systems, in line with the guidelines of General Comment No. 25 of 2021 of the UN Committee on the Rights of the Child.

The resolution, divided into six chapters, discusses essential measures to protect the interests of children and adolescents online,

aiming to guarantee their digital well-being. It also addresses the right to freedom of expression, privacy, and personal data protection.

Based on article 227 of the Brazilian Federal Constitution, Conanda emphasizes the shared responsibility among various sectors of society to provide a safe and enriching online experience for young people. This includes the commitment of the government and companies providing digital products and services to combating digital exclusion and discrimination, as well as raising awareness of both positive and negative influences of the digital world on children and adolescents.

As part of this initiative, this document also proposes the development, within 90 days of publication, of the "National Policy for the Protection of the Rights of Children and Adolescents in the Digital Environment" by the National Secretariat for the Rights of Children and Adolescents (SNDCA) and Conanda itself.



# GENERAL NEWS



## TozziniFreire Advogados hosted the event “PrivacyRules 2024 Latin American Conference”

On April 11, 2024, TozziniFreire hosted the event “PrivacyRules 2024 Latin American Conference,” organized jointly with PrivacyRules, global alliance of Privacy and Data Protection law firms. Attendees had the opportunity to talk to authorities, lawyers, Data Protection Officers (DPOs) and legal directors from companies around the world about data protection from a globalized perspective.

During the event, we had very productive discussions with the perspectives of players in different jurisdictions. For this reason, we share with you the main topics discussed:

### I. HOW TO RESPOND TO DATA BREACHES THAT AFFECT MULTIPLE JURISDICTIONS

Among the various questions about what stance companies should take in the face of data breaches with an international impact, Stephan Mulders, lawyer from the Dutch firm Van Diepen, Adriana Prado, Strategic Communication Director at FTI Consulting, and Ignacio Salguero, LatAm DPO at Chubb, highlighted relevant topics such as:

- **Collaboration between the DPO and the CISO** – collaboration between the company’s DPO and Chief Information Security Officer (CISO) is essential for effective management of the data breach

from multiple perspectives, with alignment of legal, technical, and public relations priorities with stakeholders.

- **Appointment of a PMO to align priorities** – given that a data breach requires the joint analysis and resolution from several areas of the company, a Project Management Office (PMO) should be involved to help understand the risks involved and align legal, technical, and communication priorities.
- **Communication of data breaches** – companies must be prepared to adopt strategies to communicate a violation internally and externally, to mitigate damages and manage the public's perception. Companies must understand the minimum requirements for reporting the data breach in each country with affected data subjects. They should also know if it is necessary to communicate such data breach to the competent authority(ies) and to understand the legal and administrative procedures for doing so.
- **Possible consequences and companies' liability** – companies must be aware of any possible applicable penalties and reputational consequences. It is important to adopt appropriate contractual clauses relating to possible data breaches, with a provision about compensation, as well as to conduct a complete risk assessment, to be able to demonstrate all the measures taken to comply with the GDPR (General Data Protection Regulation) and the causality and damages involved in the data breach.

## II. CHALLENGES OF IMPLEMENTING A COMPLIANCE PROGRAM FOR MULTINATIONAL COMPANIES WITH THE ENFORCEMENT OF SEVERAL DATA PROTECTION LAWS

Luiza Sato moderated the discussion between Gina Fonseca, Legal Director at Avianca, Pamela Meneguetti, Legal and Compliance Director at Nuvemshop, and María Silvana Gramaglia, VP of the LatAm Privacy Council at JP Morgan, as they shared their experiences and strategies for complying with the regulations of different countries, emphasizing the importance of an ongoing commitment to adapting and updating privacy practices.

- **Common challenges faced** – (i) knowing the privacy culture of each country involved and understanding how enforcements occur, (ii) handling and selecting partners that have the same level of commitment and maturity towards data protection, (iii) creating a data protection culture that is developed on a continuous basis for all employees and that is adapted to all the jurisdictions involved (in spite of the limited budgets for this purpose).
- **Possible solutions** – the speakers shared possible solutions such as:
  - **Obtaining corporate recognition and commitment, as well as resources allocation** – companies should have a clear and ongoing commitment from the board of directors and management to maintaining compliance with data protection laws,

as well as awareness of the importance of resources for the area.

- **Adopting compliance strategies across different jurisdictions** – creating a global system that encompasses the basic data protection principles that are common to all jurisdictions, such as the duty of transparency, accountability, respect for fundamental rights of data subjects, information security, among others, as well as prioritizing compliance with the jurisdictions of the most relevant markets and those that will process the greatest volume of data.
- **Raising awareness of the company as a whole** – raising awareness in every area and department to ensure that everyone recognizes the importance and value of personal data owned by employees, partners, and clients, and providing in-depth training to the department's managers and heads to ease the communication flows between each area and the DPO and optimize the data processing activities from the moment of data collection.

### III. ACTIONS, EXPECTATIONS, AND CHALLENGES FACED BY LATIN AMERICAN DATA PROTECTION AUTHORITIES

- **Colombian Data Protection Authority (“DPA”)** – Grenfieth Sierra Cadena, Superintendent of Data Protection in Colombia, shared the data protection regulatory landscape in the country and the initiatives that have been adopted to enhance legal security on the subject.

- In view of the 10th anniversary of the Colombian Data Protection Law, the authority stated that the law has been exercised positively and there is consolidated case law on various topics. However, they recognize the need to update their regulatory framework considering the global governance changes to ensure that there is reciprocity with other jurisdictions.
- The authority is constantly monitoring global regulatory updates to seek negotiations and collaborations with data protection authorities from other countries, as well as to issue more guidance and procedures on appropriate practices related to data processing.
- In its recommendations, the Colombian authority stated that sanctions are primarily aimed at preventing harm to society, not just punishment. To avoid penalties, data processing agents should always rely on the principles of legitimacy, consent, proportionality, and necessity when processing data, and carefully consider the risks and benefits involved in the processes.
- Finally, the Colombian judiciary branch is implementing initiatives to incorporate new technologies into its system to make it more efficient. The Colombian DPA encourages the development of new technologies, such as artificial intelligence systems, but emphasizes that these require preventive regulatory oversight and

a strengthening of security levels to ensure personal data protection.

- **Brazilian Data Protection Authority** – Kátia Cardoso, Project Manager of the Board of Directors of the Brazilian Data Protection Authority (ANPD), shared that ANPD is making further advances in negotiations with the European Union to strengthen data protection legislation in Brazil. She also demonstrated that ANPD is moving forward with the analysis of more than 800 data breaches reports and the ongoing administrative procedures, which include 4 monitoring procedures, 17

inspection procedures and 9 sanctioning procedures.

- In addition, she presented ANPD's future and ongoing work on new regulations and guidance, which include relevant topics on **(i)** processing data of children and adolescents by the government and the minimum technical security standards that must be adopted, **(ii)** data subject rights, **(iii)** Data Protection Impact Reports (DPIAs), **(iv)** communication of data breaches, **(v)** DPOs' roles, **(vi)** anonymization, **(vii)** high-risk data processing, and **(viii)** international data transfer.





## Fiesp holds event encouraging dialogue between the public and private sectors

The Federation of Industries of the State of São Paulo (Fiesp) held an event to discuss the most appropriate ways to respond to cyber incidents. The seminar was attended by the country's main data protection administrative authorities and presented experiences of both the private and public sectors.

During the event, Waldemar Gonçalves, president of ANPD, announced that later this month a resolution will be published on the Security Incident Report (CIS, in Portuguese), which will set out what organizations must send to ANPD in the case of incidents involving data subjects. In addition to clarifying essential points for cybersecurity in the country, the Resolution will also bring greater legal certainty by clearly determining the information that needs to be provided for the agency.

On the subject, Fabrício Madruga, ANPD's General Supervision Coordinator, clarified that a security incident is not just a data leakage, but also anything that could harm data subjects, such as changes to information or even the unavailability of data in systems. He said that the incident report should contain information such as how the company

handled the incident; the impacts on data subjects; the risk analysis; and the plan for communicating the incident to data subjects. Once this is done, the company's chances of facing penalties are drastically reduced, as the authority explained.

Lastly, president Waldemar Gonçalves also pointed out that all individuals, companies and organizations are susceptible to cyberattacks, so it is important not only to reinforce security, but also to train and adopt procedures to minimize damage to the organization itself and to third parties.





## Companies face pressure to meet equal pay reporting deadline

Under intense legal dispute and criticism from the government, companies with more than 100 employees are in a race against time to fill in and publish pay transparency reports, as required by the Equal Pay Act. The temporary suspension of the obligation, obtained by Fiemg, was recently revoked, triggering a race to comply with the legislation.

The president of the Regional Federal Appellate Court of the 6th Region, federal justice Monica Jacqueline Sifuentes, who suspended the effects of the injunction that exempted companies with 100 or more employees from disclosing reports on salary transparency and remuneration criteria

between men and women, stated in her decision that the names and individual data of each employee are not disclosed, so there is no harm to intimacy, privacy or Law No. 13,709 of 2018 (LGPD).

The justice also pointed out that the Equal Pay Act “reflects the commitment of the constitutional text to promoting not only formal equality, but also substantial equality, through public policies that seek to balance the gender disparities that exist in society” (case no. 6002520-79.2024.4.06.0000).

Fiemg plans to appeal the decision, expressing concerns about the exposure of sensitive data.



## Brazil makes progress in the implementation of “open health”

As with open banking, Brazil has been working to integrate information between agents in the health sector, with the implementation of the so-called “open health.”

The measure aims to gather information on the use of medical and hospital services, as well as administrative data on users, to simplify the acquisition of healthcare plans, as well as portability between healthcare companies. In addition, the integration of data is expected to reduce expenses in the health sector, enabling better resource allocation.

Since 2022, the National Health Agency (ANS, in Portuguese) has a Working Group dedicated to discussions on data integration in healthcare.

This measure is aligned with the Digital Health Strategy for Brazil, which expects data integration to be complete by 2028.

In this scenario, one of the challenges to the open health implementation will be the adjustment of information integration to the General Data Protection Law (LGPD).

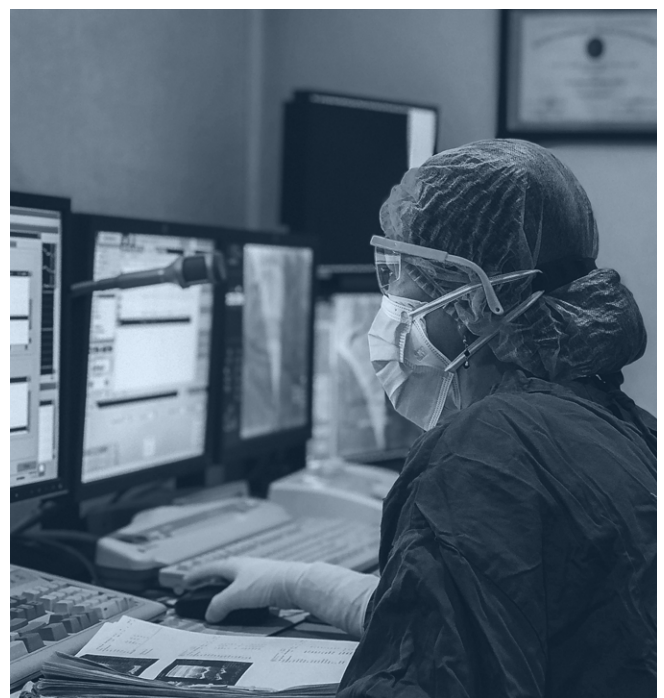
According to the LGPD, information related to health history is classified as sensitive personal data, which means that the processing of this information requires an

express and specific consent from data subjects, except in the cases provided for in LGPD.

In addition, this type of data may not be used to obtain economic advantages, except under specific conditions, which must also be observed in the information integration process.

Other challenges to be faced are the creation and adaptation of the technological infrastructure necessary for the implementation of open health, with the creation of interoperable electronic medical records and the guarantee of proper access to the internet in the whole country.

It will also be necessary to adopt robust security measures to prevent unauthorized access to the integrated personal data, in addition to cooperation between public and private health institutions operating in the country.





## Brazilian Federal Police has arrested the suspect in Brazil's largest data leakage

According to the Federal Police, the hacker investigated for leaking and selling private information of 223 million people was arrested on April 9, 2024.

The “mega-leakage” of data, which occurred in 2021, revealed personal information such as name, CPF (tax ID), photo, salary, income, education level, marital status, credit score and address of 223 million Brazilians and, at the time, both police and administrative authorities linked to consumer protection began investigations with the purpose of identifying the source of the incident.

It is also worth remembering that the National Consumer Secretariat (Senacon) and Procon-SP even notified Serasa

Experian, seeking explanations from the company regarding its possible involvement in the data leakage and to know whether the company has adopted measures to improve the security of the privacy of data subjects. The company denied that it was the source of the data and said it was cooperating with the Federal Police's investigations.

ANPD is also technically analyzing information on the incident under administrative proceeding 00261.000050/2021-59 and cooperating with the competent investigation bodies to understand the origin of the data leakage, how it took place, the measures adopted for resolution and mitigation in the contingency plan, as well as any possible effects.

# BILLS

## Bill provides for regulation of personal data monetization

Complementary Bill (PLP, in Portuguese) No. 234/2023 intends to establish the Data Empowerment General Law (LGED), which will cover the Brazilian data monetization ecosystem and which all companies that collect personal data and information and offer products or services online must formally adhere to.

PLP No. 234/2024 is being processed on an urgent basis in the House of Representatives and “aims to establish a regulatory framework for data ownership and monetization [...] that can put Brazil at the forefront in terms of dealing with the right to data privacy, data processing and the economic advantages arising from data processing and sharing within digital ecosystems.”

The PLP defines “data monetization” as the collection, analysis, grouping, processing, and commercialization of data obtained by an institution holding a data account or receiving data with the free consent of an individual or legal entity for generation of revenue or economic benefit for third parties, through online electronic platforms, internet applications, marketplaces, or data ecosystems.

If approved, the legislative proposal in question will set a pioneer global milestone by establishing rules for the monetization of data both from citizens and business entities, increasing the owners’ control over the sale of this data. This issue is not directly addressed by Brazil’s personal data protection law, known as LGPD, which is not applicable to corporate data.

The PLP has yet to receive opinions from the House of Representatives’ Committees and is currently awaiting distribution to the Science, Technology, and Innovation Committee (CCTI).



# JUDICIARY



## The Superior Electoral Court signed new agreements to combat deepfakes and hate speech in municipal elections

The Integrated Center for Confronting Disinformation and Defending Democracy has received a significant boost with the signing of agreements between the Superior Electoral Court (TSE), the Federal Police (PF) and the Office of the General Counsel for the Federal Government (AGU). The goal is to strengthen the fight against deepfakes and ensure adherence to the rules established by TSE in February for the 2024 municipal elections.

These rules were approved in February 2024, reported by the vice-president of the TSE, justice Carmen Lúcia. The main instructions against misinformation encompass the

prohibition of “deepfakes,” the regulation of the use of Artificial Intelligence in electoral advertising and the responsibility of communication platforms to remove false or offensive content.

Launched in March 2024, the Center aims to ‘*promote cooperation between the Electoral Courts, government agencies and the big techs responsible for social media platforms to prevent the spread of fake news about the electoral system and hate speech, whether of a Nazi, fascist, antidemocratic, racist or homophobic nature.*’





### 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

### 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