

TozziniFreire.
ADVOGADOS


Cybernews.

Newsletter

8th Edition | 2024

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

/European Commission will launch a public inquiry on new complementary SCCs

03 | Judiciary Branch

/Brazilian Federal Supreme Court (STF) rules that financial institutions must provide customer data to tax authorities

/ Electoral Justice innovates by enforcing data protection legislation to stop electoral campaign that used mass messaging on irregular grounds

/Superior Electoral Court (“TSE”) improperly disclosed personal data of candidates

/Cyberattacks affect STF, Anatel and PF after social media X is blocked in Brazil

/Regional Federal Appellate Court of the 6th and 3rd regions exempt companies from publishing Salary Transparency Reports

/After identifying flaws, TCU advocates for strengthening cybersecurity

/Artificial Intelligence in public data collection: Court of Justice of São Paulo decides that search engines are exempt from civil liability

04 | Administrative Authorities

/Procon-SP investigates Netshoes data leak

EDITORIAL

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

As far as the Judiciary Branch is concerned, the Federal Supreme Court (STF in Portuguese) ruled that financial institutions must provide customer data to tax authorities, affirming the constitutionality of the Confaz-ICMS Agreement No. 134.

Meanwhile, the Specialized Electoral Justice (Regional Electoral Court in Paraná) issued a relevant decision on data protection, determining the disclosure of records of personal data processing operations to investigate irregularities in the use of the database for mass messaging by a candidate.

On the other hand, the Superior Electoral Court (TSE) faced a serious data breach incident by improperly disclosing personal information of candidates, violating guidelines established by the Brazilian General Data Protection Law (LGPD). This breach, which affected the privacy of at least 70 candidates, underscores the urgent need to strengthen data protection measures in electoral processes.

Additionally, the recent suspension of social network X in Brazil triggered a

series of cyberattacks on institutions such as the STF, Anatel (Brazilian National Telecommunications Agency), and the Federal Police. These attacks not only expose the vulnerability of digital infrastructures but also reflect social tensions in the current political environment.

As regards salary transparency, recent court decisions exempted companies from publishing equal pay reports, sparking off debates about the adequacy of regulations.

Furthermore, the Federal Accounting Court (TCU) identified flaws in the Integrated Financial Administration System (Siafi) and highlighted the urgent need to enhance cybersecurity following a breach that resulted in the misapplication of government revenue.

These events reflect significant challenges in data protection and transparency in both the public and private sectors.

Finally, in the administrative scenario, Procon-SP (Consumer Protection Office) initiated an investigation into Netshoes following a leak of customers' personal data, raising concerns about compliance with the General Data Protection Law (LGPD) and the security of its users.

GENERAL NEWS

European Commission will launch a public inquiry on new complementary SCCs

The Brazilian General Data Protection Law (LGPD) and the EU General Data Protection Regulation (GDPR) have several similarities, including the requirement for data processing agents to adopt specific mechanisms to enable international transfers of personal data.

One of the mechanisms adopted by the European Commission to legitimize and ensure the protection of personal data in international transfers to third countries, in compliance with the GDPR, is the adoption of Standard Contractual Clauses (also known by the acronym SCC).

The SCCs were adopted in June 2021, but it was realized that their scope only covered international transfers made by data exporters subject to the GDPR to data importers not subject to the GDPR. This limitation ended up creating a gap for the application of SCCs in situations where both the data exporter and importer are subject to the GDPR.

To address this legal uncertainty, [the European Commission has recently announced its intention to adopt new SCCs](#)

for data transfers to data controllers and processors located outside the European Economic Area (EEA) but subject to the GDPR. This initiative is expected to be implemented **by the second quarter of 2025**, and for this purpose, the European Commission will start a public inquiry on these new clauses in the fourth quarter of 2024, so that interested parties can contribute to the establishment of these new standards.

For the drafting of the new SCCs, it will be relevant for the European Commission to consider the challenges addressed by the European Data Protection Board (EDPB) in its Guidelines, which include focusing on specific risks associated with the data importer being located in a third country, such as possible conflicts with national laws, government access in the destination country, and difficulties in enforcing rights and remedies against entities outside the European Union.

Analyzing the Brazilian scenario, in late August, **the Brazilian Data Protection Authority (ANPD) published the long-awaited first regulation on international**

data transfers, which covered the following topics: **(i)** adequacy decisions, **(ii)** standard contractual clauses, **(iii)** specific contractual clauses for certain transfers, and **(iv)** global corporate rules (see more details about this regulation [here](#)).

In this regard, when analyzing the wording of the standard contractual clauses drafted by ANPD, it is possible to notice many similarities with the wording of the European SCCs. **Both the Brazilian and European SCC models aim to ensure that the transfer of personal data to other countries complies with data protection standards**, by establishing obligations for the parties and guaranteeing the rights of data subjects and transparency.

Although the harmonization of LGPD's SCCs with GDPR's SCCs can be advantageous in many aspects, such as facilitating international cooperation, it is essential that in Brazil we still try to understand how these clauses will be effectively implemented. Many companies in the country are still developing their data protection maturity, and there may be many doubts among data exporters regarding the adoption of mechanisms that allow international data transfers.

In this scenario, **the supervision and educational work by ANPD will be crucial for companies to effectively adopt mechanisms for international data transfers**, while ensuring proper personal data protection. It is essential that ANPD consider the specificities of the Brazilian market, such as the realities of small

and medium-sized companies, which may face difficulties in meeting the SCC requirements. Additionally, the diversity in terms of technological infrastructure and access to information in different regions of Brazil demands an approach that reflects the local reality, otherwise it could hinder innovation.

Thus, **ANPD plays an important role in promoting a data protection environment that is aligned with global best practices and takes into account the specific needs and challenges of Brazil.**



JUDICIARY BRANCH

Brazilian Federal Supreme Court (STF) rules that financial institutions must provide customer data to tax authorities

The Brazilian Federal Supreme Court (STF) has reached a significant judgement on banking secrecy, affirming the constitutionality of the provisions of Confaz-ICMS Agreement No. 134, which impose on financial institutions the obligation to report information on customer transactions via PIX and cards. With a narrow 6-5 vote, the decision aims to improve the monitoring of ICMS (Tax on the Circulation of Goods and on Services of Interstate and Intermunicipal Transportation and Communication), a crucial tax for the states.

The rapporteur, justice Cármen Lúcia, argued that the rule does not represent a violation of banking secrecy, but rather a transfer of this secrecy to state tax authorities, ensuring that the data will continue to be protected and used exclusively for tax purposes. She pointed out that, with the transfer of information, tax authorities assume responsibility for keeping the privacy of the data.

On the other hand, justice Gilmar Mendes, in his dissenting opinion, warned of potential violations of the rights to privacy and

personal data protection, pointing to the lack of clear criteria on the handling and storage of this information. The justice emphasized that the rule could allow loopholes for abuse and demanded compliance with the General Data Protection Law (LGPD).

Justices Cristiano Zanin, André Mendonça, Luís Roberto Barroso and Nunes Marques sided with Gilmar Mendes.

Justices Edson Fachin, Flávio Dino, Luiz Fux and Alexandre de Moraes sided with the rapporteur, emphasizing the importance of improving tax inspection.



Electoral Justice innovates by enforcing data protection legislation to stop electoral campaign that used mass messaging on irregular grounds

The Regional Electoral Court of Paraná (TRE-PR) granted a preliminary injunction prohibiting a candidate's campaign from conducting mass sending of electoral propaganda messages. The decision also requires the candidate to stop using personal data of voters in violation of current legislation, under the penalty of a daily fine of R\$5,000 for each message sent.

Judge Mauro Henrique Ticianelli, responsible for the decision, stipulated that the candidate and the coalition must present the "Record of Data Processing Operations" of data used in the campaign within 24 hours, in accordance with the requirements of the General Data Protection Law (LGPD). Additionally, the judge set a deadline of 48 hours for the relevant Internet application providers to supply the related data and metadata.

The analysis of the data already provided suggests that the messages sent reached random recipients, including political opponents, without their consent to receive them. The judge points out that such practices may violate the LGPD, as there would be no legitimate reason for accessing personal data, and they represent an irregular use of data that undermines the equality of conditions among candidates and disrespects the rights of voters.

The decision and the imposed measure represent a landmark in the electoral area, as they are based on LGPD, addressing the improper processing of personal information. Furthermore, they illustrate how this issue—envisaged in article 33 and subsequent ones included this year 2024 in Resolution No. 23.732/2024 pertaining to Electoral Propaganda—will be interpreted and effectively applied by the Judiciary Branch.



Superior Electoral Court (“TSE”) improperly disclosed personal data of candidates

The Superior Electoral Court (TSE) improperly disclosed personal data of candidates, including CPF (Individual Taxpayer Register), sexual orientation and gender identity, disrespecting the choice of at least 70 of them who chose not to reveal this information. The flaw, corrected on August 28 after newspaper Folha was notified, occurred in the TSE’s public API, where the data was accessible for about a month, although it was not on the DivulgaCand website, which gathers information about candidacies.

The disclosure goes against a recent resolution by TSE’s president, Cármen Lúcia,

which establishes that the CPF must be kept confidential. Organizations such as Abraji have criticized this decision, saying that the CPF is essential for transparency and social control of candidacies. On the other hand, the disclosure of data on gender identity and sexual orientation, although not mandatory, aims to meet the demands of LGBTQIA+ movements for political statistics.

Experts warn that the flaw represents a violation of the LGPD, pointing out that the candidates expressly chose not to publish this information, therefore it is a double violation of the law.

Cyberattacks affect STF, Anatel and PF after social media X is blocked in Brazil

The suspension of social media X in Brazil triggered a series of cyberattacks on the systems of the Federal Supreme Court (STF), the National Telecommunications Agency (Anatel) and the Federal Police (PF). The website of the Barci de Moraes law firm, linked to the family of Justice Alexandre de Moraes, was also attacked.

The attack on the STF took place the day before the social media was suspended in Brazil, leaving systems down for less than

10 minutes. Anatel, on the other hand, reported momentary instability after the STF’s decision, but said that the systems were quickly restored. The Federal Police opened a preliminary investigation and informed that its services have been quickly normalized.

The cases are under investigation by the Federal Police, and a hacker group claimed responsibility for the attacks, which were carried out via Elon Musk’s social media, using the DDoS technique to overload the systems.

Regional Federal Appellate Court of the 6th and 3rd regions exempt companies from publishing Salary Transparency Reports

Two recent court decisions have exempted companies from publishing transparency reports, which should detail equal pay between men and women. The Regional Federal Appellate Court of the 6th Region (TRF-6), in Belo Horizonte, granted an injunction in favor of the Federation of Industries of the State of Minas Gerais (Fiemg), applicable to companies throughout the country.

Previously, on June 26, the Regional Federal Appellate Court of the 3rd Region (TRF-3), in São Paulo, granted a similar injunction to the National Union of the Machinery and Equipment Industry (Sindimaq), restricted to its members, as it understood that if companies republished the reports, this would be an “extrapolation of the normative content by the executive power.”

These decisions suspended the requirement established by Law No. 14,611 of 2023, which requires transparency reports to be published every six months on the website of the Ministry of Labor and on companies’ social media. The controversy revolves around the allegation that regulations related to publication violate the General Data Protection Law (LGPD) and go beyond legal limits.

The Office of the General Counsel for the Federal Government has not yet commented on the TRF-6 decision, while the debate about the law’s compliance with data protection rights continues, including in the Federal Supreme Court (STF), in the Direct Action for the Declaration of Unconstitutionality 7612 (ADI) submitted by the National Confederation of Industry (CNI) and the National Confederation of Commerce (CNC).



After identifying flaws, TCU advocates for strengthening cybersecurity

The Federal Accounting Court (TCU) revealed, on Wednesday (31), evidence of flaws in the Federal Government's Integrated Financial Administration System (Siafi), which is administered by the National Treasury and used for the Government's budgetary control. In April, Siafi suffered a cyberattack that resulted in the embezzlement of R\$14 million from the Ministries of Management and Innovation in Public Services and Electoral Justice.

In response to a request from the president of the House of Representatives, Arthur Lira, the

TCU said that it is cooperating with the Federal Police, the Brazilian Intelligence Agency and the Central Bank to investigate the incident. However, the official report from the National Treasury has not yet been delivered.

The TCU also reported a recent attack on the Electronic Information System (SEI), which affected several government agencies. The Court highlights the urgent need to improve cybersecurity to protect the government against attacks and minimize damage.



Artificial Intelligence in public data collection: Court of Justice of São Paulo decides that search engines are exempt from civil liability

What happened?

The Court of Justice of São Paulo ruled that information search engines, such as Jusbrasil and Escavador, are not civilly liable for disclosing data on labor cases, considering that this information is public. The dismissal of the case was upheld.

Key points:

- Public information: the court reaffirmed the publicity of judicial processes, in accordance with articles 5, LX, and 93, IX, of the Federal Constitution.
- Compliance with LGPD: there was no violation of the General Data Protection Law, since the data processed was public.
- Absence of sensitive data: plaintiff did not prove that the disclosure affected their personality rights or included sensitive information.
- CNJ Resolution: Res-CNJ No. 121/2010 imposes no restrictions on the activity of search engines.

Implications for customers:

- Chatbots and AI: services that use Artificial Intelligence to collect public data can benefit from this understanding.
- Civil liability: the decision indicates that disclosing public data does not constitute

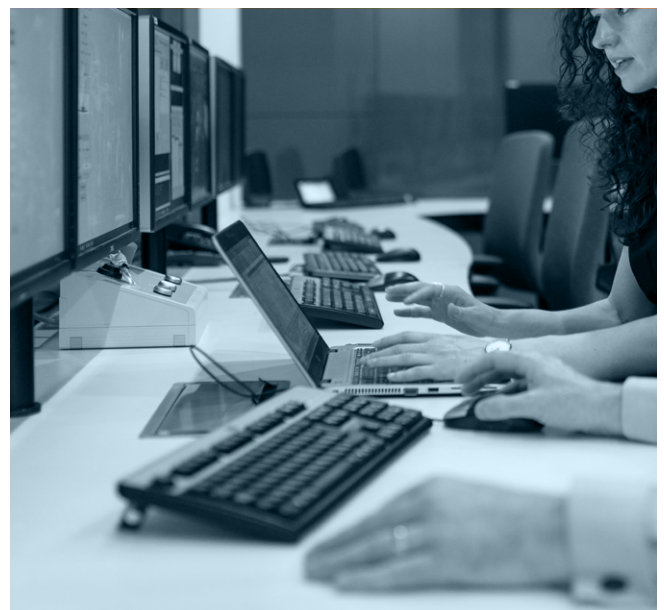
a wrongful act, as long as there is no violation of personal rights.

- Transparency and ethics: maintaining transparent practices while collecting and using public data is essential.

Recommended Action:

Clients should review their data collection practices and ensure compliance with current legislation, especially in relation to the Brazilian General Data Protection Law and potential violations of personality rights.

Case: Civil Appeal No. 1028716-35.2023.8.26.0577, rapporteur: Ferreira da Cruz. Date of judgment: August 28, 2024, Court: São José dos Campos – 5th Civil Court.



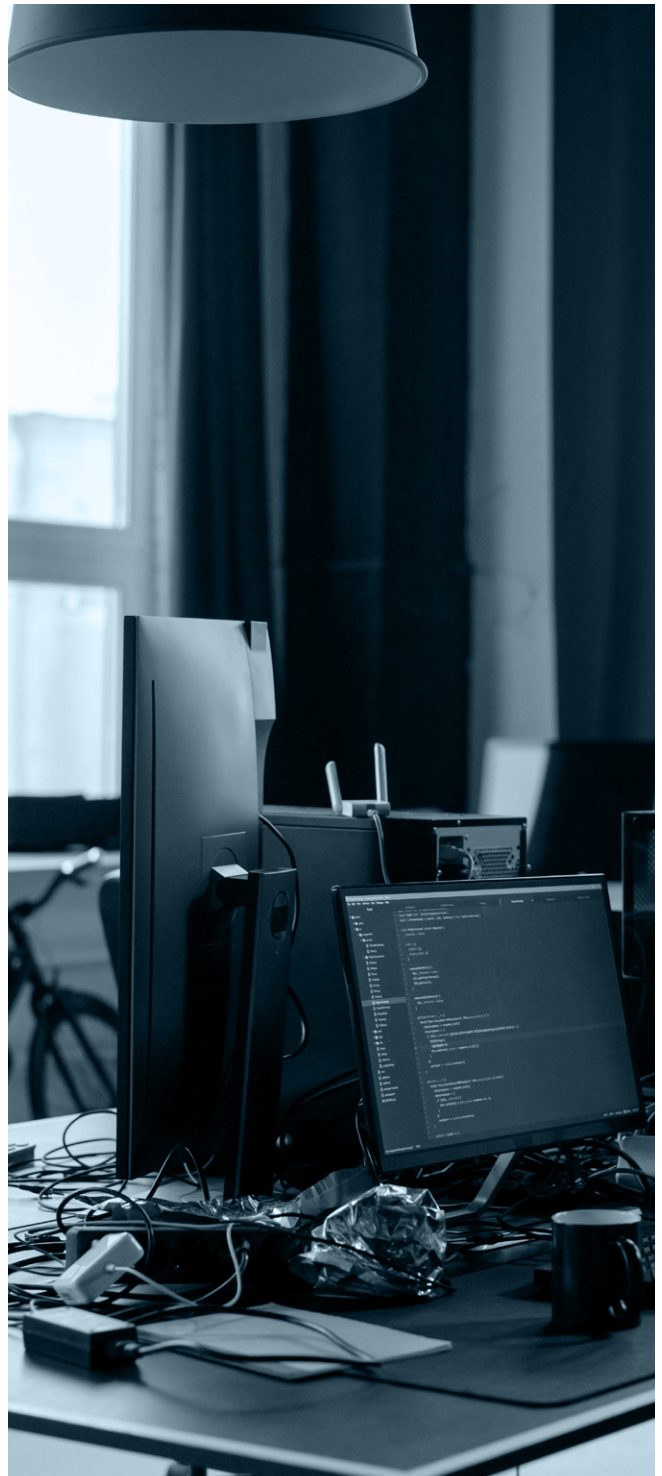
ADMINISTRATIVE AUTHORITIES

Procon-SP investigates Netshoes data leak

Procon-SP has opened an investigation into Netshoes (NS2.Com Internet S.A.) following a leak of personal customer data. The breach involved information such as names, telephone numbers, social security numbers and details of purchases made. The consumer protection office is seeking clarification on whether the company complied with the General Personal Data Protection Law (LGPD) and the Consumer Protection Code. Netshoes admitted to having been the target of a “cyber incident.”

“As soon as it was informed of the incident, Netshoes reinforced all security and control measures. [...] The company has also started a forensic investigation into what happened and will work together with competent authorities, including the National Data Protection Authority, to clarify the circumstances of the episode and avoid any setbacks for customers,” the company said.

In 2018, Netshoes had already faced a similar situation, when data of around 2 million consumers was leaked, resulting in a fine of R\$500,000.





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
- Maria Eugênia Geve de Moraes Lacerda
- Mariana Costa Alvarenga
- Miguel Lima Carneiro
- Steffani da Silva Nepomuceno