CYBER NEWS

23RD EDITION

Tozzini Freire.

ADVOGADOS

inde

01 **BRAZILIAN CONTEXT**

/ New Security Incident Reporting Form is presented by ANPD

/ Bill wants to include Brazilian Bar Association's seat on the National Council for Data Protection and Privacy

02 **GUIDELINES**

/ ICO states that immature biometric technologies could lead to discrimination

/ Slovenian Supervisory Authority establishes that the security of property can be a legitimate interest to the use of GPS tracking, if used in a proper and necessary way

03 **NORMATIVE DEVELOPMENTS**

/ EU decides to strengthen cybersecurity and resilience across the Union: Council adopts new legislation

eX.

04 JUDICIAL BRANCH

/ São Paulo Court of Justice understands that Serasa is authorized to share its consumer's telephone numbers

/ Paraíba Court of Justice understands the preservation of strategic information of a gaming company

/ For the second year in a row, an analysis regarding the application of the LGPD by Brazilian courts has been published

05 AUTHORITIES

/ Brazilian Federal Prosecution Office intends to investigate alleged deletion of computer files of the Planalto Palace

/ Most federal public bodies do not comply with the Brazilian General Data Protection Law

/ General internal affairs of the Courts have 90 days to prove adequacy to the LGPD

Tozzini Freire. ADVOGADOS

Brazilian Context.

New Security Incident Reporting Form is presented by ANPD

On December 23, 2022, the Brazilian Data Protection Authority (ANPD) made available the new Security Incident Reporting Form, which must be adopted by data controllers as of January 1, 2023.

According to the Brazilian Data Protection Law (LGPD), the data controller is obliged to report security incidents that may generate relevant risks or damages to data subjects.

Additional clarifications integrate the updated version of the form, such as the description of possible consequences and impacts of the incident and technical and administrative security measures taken before and after the incident.

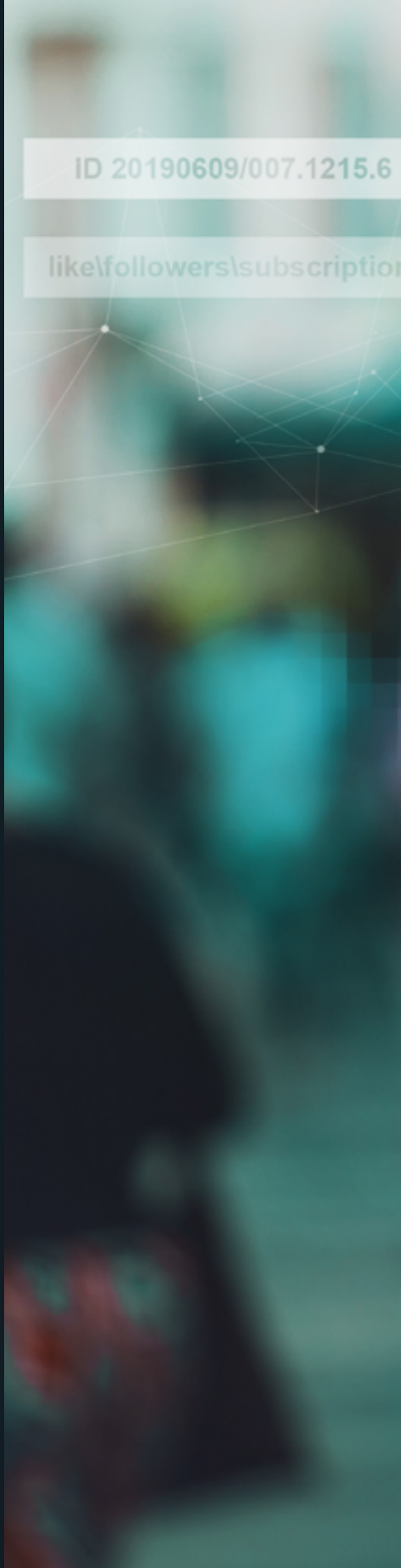
According to the current understanding of the ANPD, a security incident is any confirmed occurrence that risks the confidentiality, integrity, or availability of personal data, whether intentional – such as data theft or unauthorized access – or accidental – such as the sending of data, by mistake, to the wrong recipient.

Furthermore, in the risk assessment of an incident involving personal data, the following information must be communicated: the context of the data processing activity; the types and amount of the breached data; the potential material and moral damages to the data subjects; and the mitigation measures taken by the controller after the incident.

Bill wants to include Brazilian Bar Association's seat on the National Council for Data Protection and Privacy

Bill of Law No. 2,852/2022, filed by Senator Soraya Thronicke, aims to amend the Brazilian General Data Protection Law (LGPD) in order to create a seat for a representative of the Brazilian Bar Association (OAB), appointed by the OAB's Federal Council (CFOAB) in the National Council for Personal Data Protection and Privacy (CNPD). CNPD would then have 24 representatives. The amendment would include item XII to section 58-A of LGPD.

The Bill of Law's reasoning, according to the congresswoman, is the constitutional relevance of attorneys in Brazil, that justifies owning a seat in the CNPD, the only public collegiate body of social and multi-sectorial representation belonging to the structure of the State, with notorious social relevance.




02

Guidelines.

ICO states that immature biometric technologies could lead to discrimination

The UK Information Commissioner's Office (ICO) is concerned that incorrect analysis of biometrics and AI emotion data could result in inaccurate assumptions about a person and lead to discrimination. In the ICO's view, the only sustainable biometric deployments are those that are fully functional, accountable and backed by science.

Part of ICO's strategy is taking action against organizations that try to gain unfair advantage through the use of unlawful or irresponsible data collection technologies. The Authority is also preparing a guidance for the use of biometric data, focusing on the personal aspect of the use and collection of biometrics. The guidelines are expected to be published in the first half of 2023.

ICO believes that this will strengthen the "privacy by design" approach, in order to mitigate the risks related to biometric data and ensure that companies are operating safely and lawfully.

Slovenian Supervisory Authority establishes that the security of property can be a legitimate interest to the use of GPS tracking, if used in a proper and necessary way

On October 4, 2022, the Supervisory Authority of Slovenia decided that the use of GPS tracking may consist of legitimate interest of property security as a legal basis for processing personal data, pursuant to the provisions of Article 6.1 (f) of the General Data Protection Regulation (GDPR), as long as it is performed in an appropriate and necessary way.

In this case, after a theft at the workplace in 2009, a private sector employer introduced GPS tracking of eight of its company vehicles used by employees for delivery services. However, the tracking was done by an application that continuously, systematically and automatically recorded the location of the vehicles and consequently the location of the identifiable employees.

After investigating the case, the Slovenian Supervisory Authority decided that GPS tracking could not be used continuously but only when the vehicle is in a hazardous location and outside the employee's supervision. Otherwise, it would be an intrusive measure to the employees' privacy.

Normative Developments.

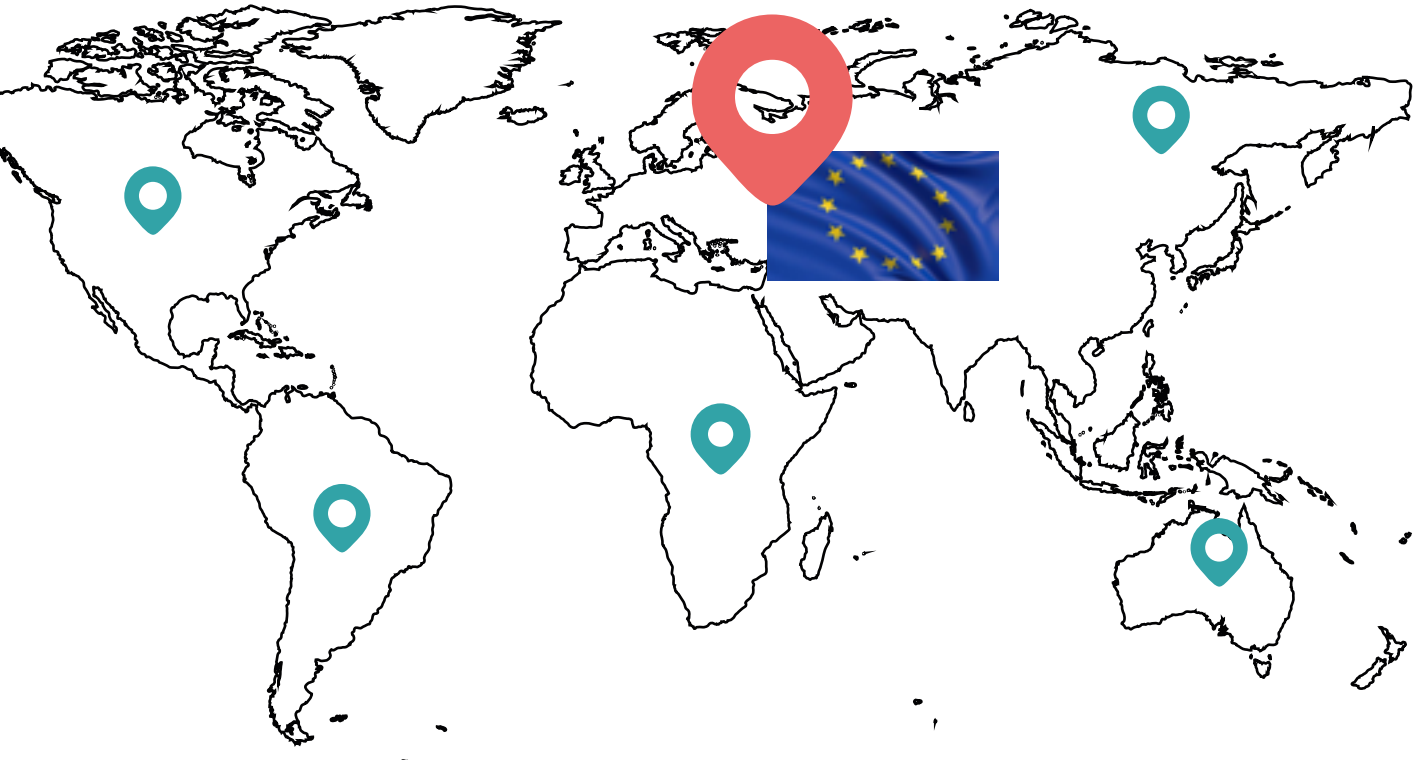
EU decides to strengthen cybersecurity and resilience across the Union: Council adopts new legislation

The Council of the European Union adopted in late November a common level of cybersecurity across the European Union by means of the new cybersecurity directive, the so-called "NIS2". The Council expects an increase of the public and private entities' ability to respond to security incidents.

The main changes brought by NIS2 include: (i) the creation of regulatory frameworks mitigating cybersecurity risks; (ii) obligation to report incidents in all sectors covered by the directive, such as health, energy, transport, and digital infrastructure; and (iii) means of cooperation between member states' data protection authorities.

Compared to the previous NIS directive, NIS2 employs a general rule to determine the entities under its regulation: all medium-sized and large entities operating in the sectors covered by the directive will be regulated by the NIS2, expressly excluding defense or national security entities, the Courts of Law, parliamentarians, central banks, among others.

NIS2 will come into force 20 days after its publication in the EU Official Gazette, and member states will have 21 months from its entry into force to incorporate its provisions in their internal legal systems.



Judicial Branch.

021

São Paulo Court of Justice understands that Serasa is authorized to share its consumer's telephone numbers

In decision published in early November, the 26th Private Law Chamber of São Paulo Court of Justice (TJSP) ruled that the disclosure of non-sensitive data for better credit protection is permitted.

The plaintiff has filed a lawsuit requesting the defendant to remove from its records information about his telephone number, as well as to compensate him at the amount of R$ 10,000.00 for moral damages. The plaintiff argued that Serasa had collected and shared with third parties his phone number without his consent, violating his right to privacy, as provided in the LGPD and the Constitution itself. The claim was dismissed, so the plaintiff appealed.

The Court upheld the decision, stating that, since the defendant is an entity whose function is to maintain a database on consumers, its conduct of selling the plaintiff's telephone number to third parties is inherent to its credit protection service, since sharing this information "**facilitates any negotiations with the consumer and provides greater security for any creditors**". Furthermore, it was understood that this information is not characterized as sensitive personal data, since the list provided in Article 5, II, of the LGPD, which provides what is sensitive personal data, does not include the telephone number. The law also allows the sharing of personal data for credit protection purposes, as occurred in the present situation, by intelligence of Articles 5, II, and 7, X, of the LGPD, together with Article 3, § 3, II, of the Positive Registration Law.

On these grounds, the Court held that Serasa is authorized to share telephone numbers with its customers without their consent, since this practice is necessary for better credit protection service.

Paraíba Court of Justice understands the preservation of strategic information of a gaming company

The Third Civil Chamber of the Court of Justice of the State of Paraíba dismissed an interlocutory appeal by understanding that the presentation of the source code of a gaming company involves disclosure of strategic information of the company.

A user has filed an action in face of a gaming company, due to the permanent suspension of its account in an electronic game owned by the company, in which they request the presentation of the source-code of the detection system, the re-establishment of their account and the unlocking of access to the game by their smartphone; or the refund of the amount spent within the game or the transfer of the "virtual goods" to a new account, in addition to the payment of compensation for moral damages.

In first degree, the judge has ordered the defendant to meet the plaintiff's request, presenting at the court the source code of its system, with the conclusions of the algorithm used by it, as well as the data of the players who allegedly denounced the plaintiff in the game.

The Court understood that the decision cannot prevail, because it involves the disclosure of strategic information that should be kept confidential for the protection of the business activity developed by the company.

For the second year in a row, an analysis regarding the application of the LGPD by Brazilian courts has been published

The Brazilian Institute of Education, Development and Research (IDP) and the Jusbrasil portal – with support from the United Nations Development Program (UNDP) – have published a new analysis with a selection of the most important judicial decisions involving the Brazil's General Data Protection Law (LGPD) for the second consecutive year.

The research was carried out through an artificial intelligence system that allowed the analysis of 1,789 documents of the Brazilian justice system – among different official electronic journals and case law – that involved the use of the LGPD, between September 2020 and September 2022. The Courts of Justice of the State of São Paulo, Bahia, Rio Grande do Sul, and the Federal District were the ones that stood out.

By following the evolution and maturation of the Brazilian General Data Protection Law (LGPD), it has been noted its mention in different areas of law, with emphasis on Consumer, Civil, and Labor Law. Comparing to its first year of validity, the application of the LGPD is likely to increase, considering that in 2021, 274 court decisions were identified and, in 2022, 665 decisions in which relevance in the discussion involving the LGPD were seen.

Finally, the most recurrent topics in which the LGPD was discussed were: (i) requests for digital evidence of geolocation in labor lawsuits; (ii) civil liability for security incidents and data leakage; (iii) undue enrollment in the Serasa defaulter register; and (iv) right to review the automated processing of personal data.

Authorities.

Brazilian Federal Prosecution Office intends to investigate alleged deletion of computer files of the Planalto Palace

After news that HDs of equipment of the Presidency of the Republic would be being formatted because of an alleged threat to systems and databases, Federal prosecutors requested investigative process involving possible deletion of computer documents of the Planalto Palace, warning that the facts are serious and sufficient to establish an investigation.

The ministerial body requests that the General Secretariat explain who determined the formatting of the hard drives and whether possible causes and persons responsible for the event were investigated. It is also argued that the Presidency did not clarify whether computers were formatted, if files were damaged or deleted, if sensitive data were leaked, if public data were lost, or if there was an investigation into the origin of the attack.

The General Secretariat, in turn, assured that there was no leak of data or compromise of systems hosted on the network of the Presidency of the Republic, informing that it had detected "malware" on some computers, which would have originated from the practice of "phishing".

Most federal public bodies do not comply with the Brazilian General Data Protection Law

In a recent agreement, the TCU revealed worrying data regarding the degree of adaptation of federal public bodies in relation to the LGPD.

According to the data collected in audits of 382 federal public institutions carried out by the Federal Court of Auditors, it concluded that 76.7% of the institutions are at an insignificant or initial level of improvement to the LGPD. In addition, 82% of entities do not consider the risks of exposure to security incidents when processing data of Brazilian citizens.

The result is surprising because the expectation was that the administrative sanctions of the ANPD, which depended on a specific Ordinance regarding the dosimetry of penalties related to the LGPD, would start to be applied by the competent administrative authority in October 2022.

In addition, the information gains more relevance if considered together with the fact that Brazil is a recurring victim of virtual attacks, such as the one that occurred in December 2020 against the Ministry of Health (mentioned in the Brazilian Court of Accounts report), in which the data of more than 223 million Brazilians were exposed.

General internal affairs of Courts have 90 days to prove adequacy to the LGPD

The General Internal Affairs of the State Courts of Justice must, within 90 days, provide clarifications on the adequacy to the General Law of Data Protection.

The purpose is to put into practice Provision No. 134/2022 of the national internal affairs, which provides for measures to be adopted by extrajudicial notaries to adapt to the General Law of Data Protection. As an example, the Provision states that those responsible for registry offices must pay attention to technical and administrative security measures to protect personal data from unauthorized access or accidental or illegal situations that may violate the appropriate treatment of the data.

The adequacy is important because of the vulnerability of the information that is provided to the agents responsible for the civil registry offices of natural persons.

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