# Tozzini Freire. ADVOGADOS

CYBERNEWS.

26<sup>th</sup> Edition

### index



01	BRAZILIAN CONTEXT		04	AUTHORITIES	
		5			14
		7			14
02	GUIDELINES		05	NORMATIVE DEVELOPMENTS	
		9			<u>1</u> 6
03	JUDICIAL BRANCH				17
		11	05	INTERNATIONAL RULINGS	19
		12			





# Brazilian Context.

Brazilian Data Protection Authority publishes its regulation on the rules for applying LGPD penalties

On February 27, 2023, the Brazilian Data Protection Authority (ANPD) published Regulation on the **Application** Calculation and of Administrative Sanctions as an additional step towards ensuring the enforceability of the Brazilian General Data Protection Law (LGPD). As its primary objectives, the Regulation aims to establish standards and criteria for the application of administrative sanctions by the ANPD, as well as to define the form and calculation methods for the base value of fines.

It should be noted that the LGPD sets forth a list of possible sanctions, which include warnings, suspension of the use of the affected personal databases, public disclosure of the infraction, and the application of a fine of up to BRL 50,000,000.00 (fifty million Brazilian reais, currently around 9.5 million dollars), among others.

According to the Regulation, sanctions will be applied proportionally to the violation, which can be classified as light, medium, or severe. Such classification takes into account 11 criteria that include

an analysis of (i) the severity and nature of the violations and the data subjects' rights that were affected, (ii) the level of damage incurred, (iii) the offender's good faith, (iv) its economic condition, and (v) the potential advantage gained or intended to be gained from the violation. Additionally, ANPD will consider to what extent the agent has implemented a (vi) prompt corrective measure and whether (vii) internal mechanisms and procedures were set in motion to mitigate the damage.

Concerning monetary sanctions, the definition of the initial value of the fines will be grounded on an objective methodology provided for in the Regulation. For this calculation, the Authority will consider (i) the classification of the violation, (ii) the level of the identified damage, (iii) the offender's revenues, as well as any (iv) mitigating and aggravating circumstances present in the violation.

About a month after the

publication of the Regulation, we have already noticed that the application of sanctions non-compliance with the LGPD is effective: ANPD has filed eight administrative proceedings involving mostly federal public sector bodies, such as the Brazilian Health Ministry, the Federal District Education Secretariat, and the Santa Catarina State Health Secretariat, for alleged data breach, lack of notification of security incidents, failure to appoint a DPO, lack of Records of Processing Activities (ROPA), and data protection impact assessment and/or failure to comply with ANPD requests. All of them are currently in the investigation phase and are about to be judged.

The ANPD has published the list of these proceedings, which contains the name of the public agency or private company, the undertaken conduct, the sector in which it operates, the stage of the process, and the number of the proceeding filed before ANPD. However, the penalties that will be applied for each case

and access to the documents in the process will only be publicly available after the conclusion of the investigation.

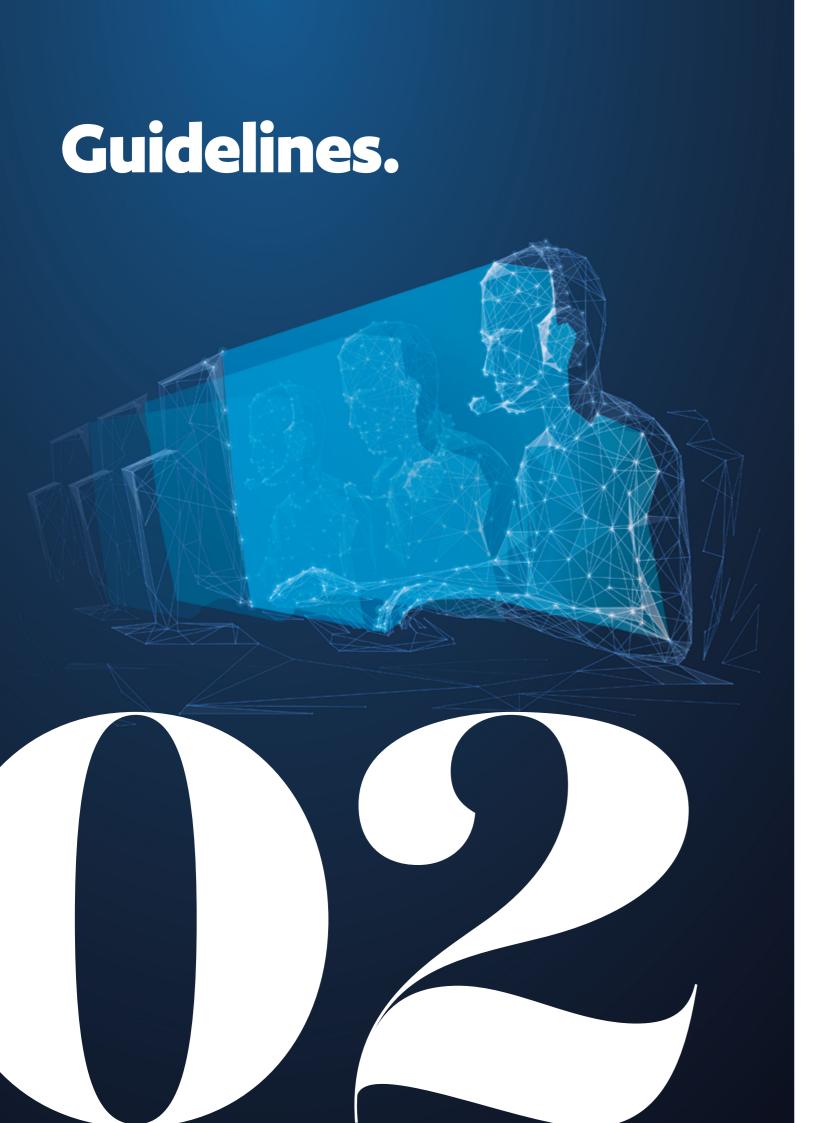
Finally, although the first cases mostly involve the public sector, the ANPD's director, Nairane Leitão, explained that this is not the only target of the enforcement actions, being there also a second set of cases involving private companies with violations beyond data breach, such as undue selling and sharing of data.

The full Regulation is available here.

### ANPD publishes a technical note regarding the application of the LGPD for deceased persons

On March 17, 2023, the ANPD published a technical note taking a position on the non-application of the LGPD in the case of processing data of deceased persons.

The justification is based on Article 6 of the Brazilian Civil Code, according to which the existence of a natural person ends with the death. Therefore, it is assumed that the incidence of the LGPD occurs only in the context of the processing of personal data of living natural persons.



### New Guidance on game development and child protection issued by the ICO

The United Kingdom's Data Protection Authority, the Information Commissioner's Office (ICO), has drafted a new guidance, aiming at the gaming industry. The guidance addresses the protection of children from online risks and focuses on how game developers, publishers, and platform operators should comply with the General Data Protection Regulation (GDPR) and the UK's Data Protection Act 2018 (DPA 2018).

Some of the provisions of the new guidance include drafting Data Protection Impact Assessments (DPIA), to evaluate the risk of processing children's personal data. In addition, the guidance suggests the exhibition of clear information on how data are processed and the collection of a valid consent from the kids' parents or legal guardians.

The guidance encourages game developers to design the games in a way that guarantee children's rights to privacy and prevent them from carelessly exposing their personal data, so that it can offer a safer gaming experience for underage players.

## Judicial Branch.



### Brazilian Federal Supreme Court rules on the provision of user data by digital platforms

After a long period of suspension, the judgment of the ADC (Action for the Declaration of Constitutionality) No. 51, which aims to analyze the constitutionality of the MLAT (Mutual Legal Assistance Treaty in Criminal Matters), was finally summed up on February 23, 2023.

As per the majority opinion, Minister Gilmar Mendes along with most of the other Justices have ruled on the constitutionality of the MLAT, without prejudice to the direct application of Article 11 of the Civil Rights Framework for the Internet (Law No. 12,965/2014). It determines that Internet application providers must provide information to Brazilian authorities regarding data collected in Brazil.

The controversy of the lawsuit was regarding the main allegations from technology companies, which do not have servers in Brazil, claiming that were submitted to the American laws for disclosing content. They also allege that Brazilian authorities have resorted to the mechanisms of judicial cooperation of the MLAT, in order to, in contact with American authorities, request the contents of users.

The Supreme Court stated that the judicial cooperation mechanisms provided for in the MLAT should be applied in cases where technology companies are not headquartered in Brazil, nor do they have subsidiaries in the national territory. In cases where companies have branches in Brazilian territory, the Justice understands that the direct request of data from technology companies is constitutional, without the need for communication with the American authorities.

#### Brazilian Superior Court of Justice holds that leak of non-sensitive personal data does not generate presumed moral damages

or Court of Justice (STJ), reversing third party would not violate the the decision handed down by the personality rights of the holder. Court of Justice of the State of São Paulo (TJSP), held that the leak of Furthermore, the vote confirmed personal data does not have the understanding that, although power to generate compensable the failure in the treatment of permoral damages, being necessary sonal data by a legal entity is repto prove the damage resulting rehensible, the leaking of such data from exposure of the information does not, in itself, entail compensaby the data holder.

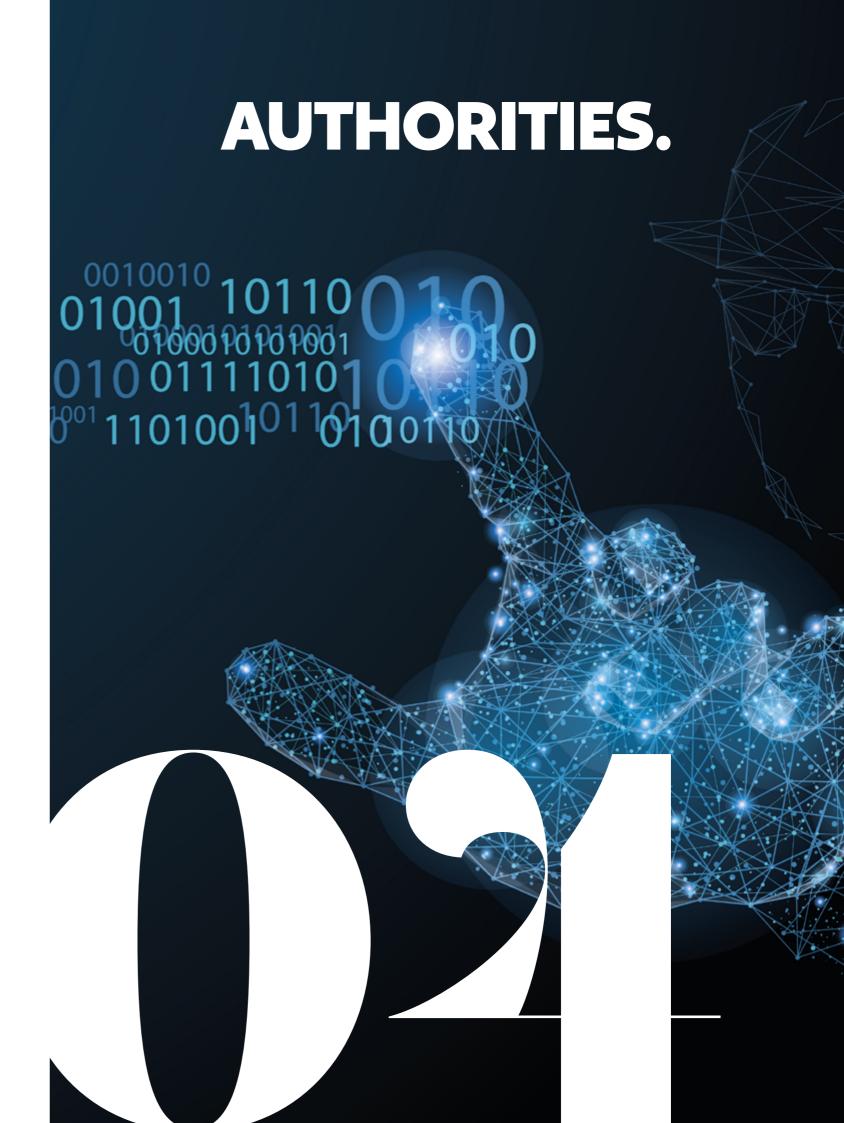
sentence had been reformed to sumer proves any possible damcondemn the electric utility com- age resulting from the exposure of pany ENEL to pay moral damag- this information, which is characes to the data holder. However, terized as non-sensitive data. consumer.

data are provided on a routine ba- erability. sis, the reporting judge understood

The Second Panel of the Superi- that knowledge of such data by a

ble moral damages. As it is not a question of presumed moral dam-At the state court, the first-degree ages, it is necessary that the con-

as argued by the company in the This is the first precedent of the special appeal, the leaked data do STJ on compensation for data leak not qualify as sensitive under the based specifically on the legal pro-LGPD, so the leak could not, by it- visions of the LGPD and will guide self, cause moral damage to the the jurisprudence on the subject. This understanding confirms the The central premise adopted by keynote of recent judgments althe reporting judge Francisco Fal- ready issued by the Court, in the cão was that the data reported as sense that the trivialization of morleaked would not be sensitive, since all damages must be avoided, given they are registration data, such as that the compensation in this re-CPF (Brazilian Individual Taxpayer gard must take into consideration Registry), telephone number, and whether there was effective damaddress, for example. As these age that exceeded the limits of tol-



#### **Brazilian Post Office informs** data leakage of personal data

Last month, due to technical flaws in the application "My Post Office", personal information was leaked, such as phone numbers and register number.

After detecting the incident, the organization sent a statement to the Brazilian National Data Protection Authority (ANPD) and provided new security measures.

The company did not disclose

the exact number of accounts exposed nor what led to the technical flaws, but the impact reached 5% of all registrations. They warned that the vulnerability could allow cybercriminals to relate a register number to a registered cell phone number.

Given this, the Post Office advised all its users to change their passwords for access to the application.

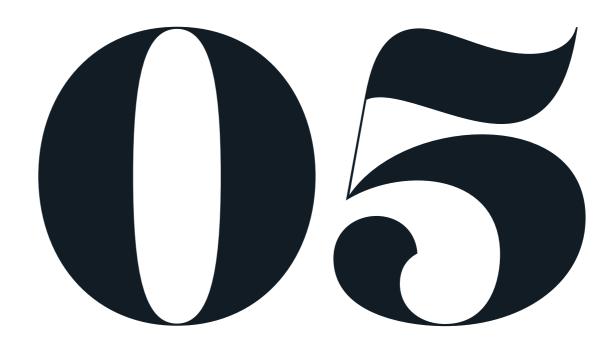
Brazilian Public Prosecutor
Office notifies users about a
possible data leak

The Federal Public Prosecutor Office (MPF) sent an e-mail alert to users of its "MPF Electronic Protocol" system, notifying them of a possible leak of non-sensitive data, such as name, e-mail, phone number, and IP address.

No sensitive information capable of generating false profiles or identity theft and fraud was leaked. The concern here is the use of this information to scam users of the MPF system.

The public agency, in addition to emailing users informing them of the security incident, has also notified the ANPD (National Data Protection Authority) and taken the necessary measures to stop possible improper access and prevent further incidents.

There is no evidence that the data has used or been using for inappropriate or illegal purposes.



# Normative Developments.

14

#### **EU Council elaborates document to** clarify the Cyber Resilience Act's interplay with AI and product safety Acts

published, through the Swedish acts are relevant pieces of the presidency, clarifying the correlation the Artificial Intelligence Act, information on how and the Product Safety Act. Cybersecurity Act and This new document is focused Artificial the abovementioned acts in conformity strategy sector.

concept of "cybersecurity applicable penalties. resilience" in a decade of increasing cyber threats and

The European Union Council has security incidents. The three document network security framework.

between the Cybersecurity Act, Also, the document provides the Intelligence Act on the ways to implement will come into force, the assessment the cybersecurity and digital and which products will have to be submitted to the data protection authorities -, the The document explores the enforcement rules, and the

#### Ransomware may be included as a crime in the Brazilian Penal Code

The Bill of Law No. 879/2022, If approved, the Bill of Law will years, to 2 to 5 years plus a fine criminal law in force in Brazil". (Criminal Code, section 154-A, paragraph 3)

drafted by Senator Carlos Viana addthe "kidnappingofcomputer (PL/MG), proposes to amend data" as a crime, with possible the Brazilian Criminal Code qualifiers. The Senator justifies (Decree-Law No. 2,848/40) the Bill of Law by claiming that to include section 154-C. The the recurrence of ransomware amendment would include an attacks - both on individuals additional crime to section IV and government agencies urges of the Criminal Code, which - "(...) the creation of a specific addresses crimes against the crime to discourage the practice inviolability of secrets. The of the conduct popularly called Bill of Law also increases the 'data kidnapping', a type of penalty in case of invasion of cyberattack that is not yet a computer device from 1 to 4 perfectly subsumed by the

17

16



#### The French SA fines **DISCORD EUR 800.000**

(GDPR). This is the result of an ties. investigation from CNIL concerning Discord's cookies practices Along with the fine, CNIL ordetion on how they are used.

The French Data Protection to its users about the data pro-Authority (CNIL) issued a EUR cessing activities being carried 800,00 fine against Discord, a out on the platform. The French communication and instant authority also concluded that messaging platform, for fai- Discord did not obtain valid ling to comply with the Gene- consent from users to carry out ral Data Protection Regulation certain data processing activi-

and the lack of clear informa- red that Discord amends and improves the company's data processing activities to comply Discord is accessed by millions with the GDPR. The measures of users worldwide. According include implementing a valid to CNIL, the company did not consent management tool and provide adequate information providing clear information on

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

