

Tozzini Freire.

ADVOGADOS

CYBERNEWS.

26th Edition

index

CYBERNEWS 26th EDITION

01	BRAZILIAN CONTEXT	5
		7
02	GUIDELINES	9
03	JUDICIAL BRANCH	11
		12

04	AUTHORITIES	14
		14
05	NORMATIVE DEVELOPMENTS	16
		17
05	INTERNATIONAL RULINGS	19

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 its Regulation on the Calculation and Application 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 for 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.

Guidelines.



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

The Second Panel of the Superior Court of Justice (STJ), reversing the decision handed down by the Court of Justice of the State of São Paulo (TJSP), held that the leak of personal data does not have the power to generate compensable moral damages, being necessary to prove the damage resulting from exposure of the information by the data holder.

At the state court, the first-degree sentence had been reformed to condemn the electric utility company ENEL to pay moral damages to the data holder. However, as argued by the company in the special appeal, the leaked data do not qualify as sensitive under the LGPD, so the leak could not, by itself, cause moral damage to the consumer.

The central premise adopted by the reporting judge Francisco Falcão was that the data reported as leaked would not be sensitive, since they are registration data, such as CPF (Brazilian Individual Taxpayer Registry), telephone number, and address, for example. As these data are provided on a routine basis, the reporting judge understood

that knowledge of such data by a third party would not violate the personality rights of the holder.

Furthermore, the vote confirmed the understanding that, although the failure in the treatment of personal data by a legal entity is reprehensible, the leaking of such data does not, in itself, entail compensable moral damages. As it is not a question of presumed moral damages, it is necessary that the consumer proves any possible damage resulting from the exposure of this information, which is characterized as non-sensitive data.

This is the first precedent of the STJ on compensation for data leak based specifically on the legal provisions of the LGPD and will guide the jurisprudence on the subject. This understanding confirms the keynote of recent judgments already issued by the Court, in the sense that the trivialization of moral damages must be avoided, given that the compensation in this regard must take into consideration whether there was effective damage that exceeded the limits of tolerability.

AUTHORITIES.

0010010
01001 10110 010
0100010101001
0100111101010
1001 1101001 0100110



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 neces-

sary 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.

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

The European Union Council has published, through the Swedish presidency, a document clarifying the correlation between the Cybersecurity Act, the Artificial Intelligence Act, and the Product Safety Act. This new document is focused on the ways to implement the abovementioned acts in the cybersecurity and digital strategy sector.

The document explores the concept of “cybersecurity resilience” in a decade of increasing cyber threats and

security incidents. The three acts are relevant pieces of the network security framework.

Also, the document provides information on how the Cybersecurity Act and the Artificial Intelligence Act will come into force, the conformity assessment – and which products will have to be submitted to the data protection authorities –, the enforcement rules, and the applicable penalties.

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

The Bill of Law No. 879/2022, drafted by Senator Carlos Viana (PL/MG), proposes to amend the Brazilian Criminal Code (Decree-Law No. 2,848/40) to include section 154-C. The amendment would include an additional crime to section IV of the Criminal Code, which addresses crimes against the inviolability of secrets. The Bill of Law also increases the penalty in case of invasion of a computer device from 1 to 4 years, to 2 to 5 years plus a fine (Criminal Code, section 154-A, paragraph 3)

If approved, the Bill of Law will add the “kidnapping of computer data” as a crime, with possible qualifiers. The Senator justifies the Bill of Law by claiming that the recurrence of ransomware attacks – both on individuals and government agencies urges – “(...) the creation of a specific crime to discourage the practice of the conduct popularly called ‘data kidnapping’, a type of cyberattack that is not yet perfectly subsumed by the criminal law in force in Brazil”.

International Rulings.



06

The French SA fines DISCORD EUR 800.000

The French Data Protection Authority (CNIL) issued a EUR 800,00 fine against Discord, a communication and instant messaging platform, for failing to comply with the General Data Protection Regulation (GDPR). This is the result of an investigation from CNIL concerning Discord's cookies practices and the lack of clear information on how they are used.

Discord is accessed by millions of users worldwide. According to CNIL, the company did not provide adequate information






to its users about the data processing activities being carried out on the platform. The French authority also concluded that Discord did not obtain valid consent from users to carry out certain data processing activities.

Along with the fine, CNIL ordered that Discord amends and improves the company's data processing activities to comply with the GDPR. The measures include implementing a valid consent management tool and 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

**Tozzini
Freire.**
ADVOGADOS