

Tozzini Freire.

ADVOGADOS

CYBERNEWS.

30th Edition | 2023

Index

01

.....	03
.....	03
.....	04
.....	04
.....	05

02

.....	06
.....	08
.....	09
.....	10

03

.....	11
-------	----

04

.....	12
-------	----

05

.....	13
.....	14



Brazilian Context.

Public inquiry on international personal data transfers is opened by ANPD

On August 15, a public inquiry was opened by the Brazilian Data Protection Authority (ANPD) on the draft Resolution regarding the Regulation of International Personal Data Transfers and the model of Standard Contractual Clauses, in compliance with articles 33, II, subitems a, b and c, art. 35, paragraphs 1, 2 and 5, and art. 36 of the Brazilian General Data Protection Law (LGPD).

The inquiry will be available until the 14th of September.

Inquiry among society on preliminary study regarding Legitimate Interest is opened by ANPD

On August 16, the ANPD opened an inquiry among society on the Preliminary Study regarding the legal hypothesis of processing personal data of legitimate interest, provided for in art. 7, IX of the LGPD.

The study aims to support the content of the Guide on the legal hypothesis of legitimate interest, by combining the Authority's technical expertise with the processing agents' practical experience in the subject.

New identity card will use blockchain

The Brazilian government has decided to adopt the blockchain authentication and encryption system in the new identity card, which will replace the Brazilian ID (RG) number with the Individual Taxpayer Registry (CPF) as a unique identifier number valid in the national territory.

The information was conveyed by the Secretary of Digital Government of the Ministry of Management and Innovation, Rogério Mascarenhas, who said that the innovation aims to prevent counterfeiting, by ensuring that the information is valid.

Bill of Law proposed to make it mandatory to disclose personal data security breaches in the media

If Bill 1,876/2023, submitted by federal deputy Marcos Tavares is approved in the thematic committees of Communication and Constitution, Justice, and Citizenship, disclosing data breaches that may entail relevant risk or damage to data subjects may become mandatory in widely circulated media vehicles.

The Bill will also require data processing agents to disclose information about the data breach in their social media and internet profiles, in addition to the already mandatory report to the Brazilian Data Protection Authority (ANPD). In addition, the Bill makes it possible for the Executive Power to create supplementary rules to enforce the new obligation.

The congressman believes that the measure will be positive to give more transparency on data breaches.

ANPD Board of Directors sends list of candidates for the 2nd formation of CNPD to the Presidency of Brazil

On July 28, the Brazilian Data Protection Authority (ANPD) shared with the President the shortlists formed by the ANPD's Board of Directors for the 2nd Formation of the Brazilian Data Protection Council ("CNPD"), so he may assess the list. The new council members will be appointed by the President throughout this year for a two-year term working alongside the ANPD.

The CNPD is structured as an advisory body connected to the ANPD, aimed at involving civil society and the public sector in the discussions held by the Authority. With this goal, the CNPD opened specific applications for five different groups, including: (i) civil society organizations, (ii) scientific, technological, and innovative institutions, (iii) trade union confederations, (iv) representative entities of the business sector, and (v) representative entities of the labor sector.

In this scenario, the CNPD plays a critical role in shaping policies and practices related to personal data protection and privacy in Brazil, thereby seeking to ensure the effective implementation of the LGPD in direct support of ANPD.



02

Judicial Branch.

Companies ordered to pay damages due to hacker attack

A credit card processing company is ordered to pay damages due to negligence in adopting security measures. The decision was rendered by the 2nd Appellate Panel of Santa Catarina Court of Justice (TJSC), which understood there was concurrent fault in a hacker attack.

According to the complaint, in November 2021, a company operating in the wholesale and retail segment entered into a contract with a company responsible for managing credit card payment machines. On January 14, 2022, employees of the wholesale and retail company noticed that the system had been hacked, resulting in the unauthorized transfer of BRL 3,900.00 thousand reais to an individual who was not part of the staff.

In view of this event, the company that was the victim of the attack filed an action for pecuniary damages against the credit card processing company, seeking reimbursement for the improper transfer. The company responsible for the machine, however, claimed that the fault was exclusively of third parties that hacked the system and questioned the applicability of the Consumer Protection Code (CDC) to the case.

The court then unanimously upheld the judgment of the Small Civil Claims Court of São Miguel do Oeste Civil (TJSC), which ruled that both companies were at fault in

the incident. As a result, the company responsible for the credit card machines was ordered to pay half of the loss, totaling BRL 1,950 thousand reais.

The Court noted that the damaged company had been negligent by failing to implement an adequate firewall system to protect the network and ensure the identification of those who accessed the system. It also recognized that the security provided by the system available was below expectations, due to the use of weak passwords and the lack of specific monitoring of the IPs that accessed the device.



Both businesses and consumers are responsible for personal data protection

A judge from Goiânia issued a decision determining that data protection requires caution from both sides – from companies, when creating security policies and measures, and from users, in keeping their personal data and passwords protected.

The 5th Small Civil Claims Court of Goiânia denied the moral damages sought by a consumer, who claimed that an airline company had leaked her personal data.

The plaintiff argues that her former steady union is subject of a lawsuit, and that her ex-spouse brought to the records of this case, without her consent, information about the tickets of the trip she made to Portugal, which violates her personal data.

However, judge Roberta Nasser Leone understood that there was carelessness of the plaintiff herself, after all, this information could only be obtained from her login and password, so there is no way to prove any data leakage by the defendant company.





TJSP states there is no violation of the LGPD when public data are processed

In trials held at the end of July and the beginning of August, the Court of Justice of the State of São Paulo (TJSP) stated that, when the information contained in the database is public and obtained by lawful means, processed for credit protection, there is no indemnifiable illicit act. The decision is in line with article 7, item X, of the LGPD, Brazilian General Data Protection Law.

In addition, the Court also understood that when the data disclosed are merely registration data, not constituting sensitive data, there is no breach of the duty of information, since there is no need for authorization or communication from the subject of those personal data.

In this sense, in March 2023, the Superior Court of Justice also ruled that there are no damages for pain and suffering in the event of leakage of merely registration and non-sensitive data, such as social security numbers and telephone numbers, since these are data that are provided routinely and would not have the power to violate the data subject's right to personality.

Brazilian Data Protection Authority filed a public interest civil action to protect its identity in favor of the common interest

ANPD filed a public interest civil action alongside the Brazilian Patent and Trademark Office (BPTO) against the National Association of Data Privacy Professionals (ANPPD) and its president, in order to cease the use of name, brand, and acronym homophones to those of ANPD.

According to ANPD, the use of these identifying signs are confusing companies, professionals, and consumers, and thus constitutes misleading advertising. The association ends up pretending to be a government entity and, therefore, poses a risk to society as a whole.

In addition to the irregularities in nominal and visual identification, ANPPD also created, without legal authorization, a National Register of Data Privacy Professionals and claims to be in charge of approving privacy software and courses on Data Protection.

After investigating the issues mentioned above, the BPTO decided that the registration of acronym ANPPD, which had previously been made, should be revoked and made null. It turns out that, as more than 180 days had passed since the registration was made, nullity can no longer be declared at the administrative level. Thus, an interlocutory relief was filed to cease such harmful practices.

The interlocutory relief was granted determining that (i) the publication of advertising regarding the National Register of Privacy Professionals and the respective National Register of Data Privacy Professionals is suspended; (ii) the association refrains from using acronyms and logos similar to those of ANPD, even if in the form of visual identity, in the association's corporate name and in social media and other means of communication linked to the association and to the members of the boards (it is also required to modify and/or remove any previous posts); and that (iii) the association refrains from using the domain name anppd.org, which must be changed within 120 days.

In the decision, the judge recognized that the similarities between the identifying signs of ANPD and ANPPD are indeed noticeable, either through the acronyms, the colors used or the corresponding areas of activity, which can cause confusion and damage to the consumer market, justifying, therefore, the interlocutory relief granted to suspend ANPPD's use of similar acronyms and logos.

03 Authorities.

State of Goiás presents a Bill to prevent establishments from requesting personal data from consumers for sales purposes

Goiás State Senate is studying a Bill (600/23) that would prohibit commercial establishments from requiring consumers to provide personal data as a condition for sales or provision of services.

According to the Bill, “commercial or service establishments are prohibited from making the sale of products or the provision of services conditional upon the provision of personal data by consumers, except in cases where the obligation to provide such data is determined by law.” The matter was approved by the Commission on Constitution and Justice (CCJ) and will be voted on the floor.

Under the proposal, whose author is state representative Vetter Martins, failure to comply with the measure would subject violators to the sanctions provided for in the Consumer Protection Code, except in cases where data provision is mandatory under the law.

To justify the bill, the state representative claims that the measure seeks to bring more clarity to consumers and is in line with the guidelines of the Brazilian General Data Protection Law.

021

Normative Developments.

CNI publishes a guide of good practices on personal data protection for use in industries

The Brazilian National Confederation of Industry (CNI) published an extensive guide of good practices on personal data protection for use in industry processes (please access it [here](#)). Moreover, it highlighted that the implementation of a data protection culture in industries increases customer loyalty and trust, expands business opportunities involving personal data and contributes to compliance with legal requirements.

To encourage and assist industries to comply with LGPD, the guide highlights the main concepts and principles of LGPD, provides examples of processes and types of personal data processed by the industry sector, as well as general protocols for each stage of data processing, from data collection to elimination. In addition, the guide presents specific protocols for the marketing area of industries, international data transfer, and for the fulfilment of LGPD's legal obligations, such as the preparation of data protection impact assessments and guarantee of data subjects' rights.

05

International Rulings.

French Data Protection Authority fines Criteo €40,000,000

On June 15, 2023, the French Data Protection Authority (CNIL, in French) imposed a EUR 40 million fine against an online advertising company specialized in behavioral retargeting (tracking users' browsing through cookies to display personalized advertisements), for failing to comply with the General Data Protection Regulation (GDPR). This fine is the result of a CNIL investigation into Criteo's failure to collect consent from data subjects.

Criteo also failed to comply with other provisions of the GDPR regarding the obligation of information and transparency, ensuring the data subject's right of access, revocation of consent and data elimination, and failure to provide for an agreement between data joint controllers (articles 7.1, 7.3, 12, 13, 15.1, 17.1 and 26).



India passes new digital data protection law

In August, India approved the Digital Personal Data Protection Law, which establishes rules and procedures for personal data processing carried out by tech companies.

Among its provisions, the law, in short, (i) gives the government of India powers to exempt state agencies from the law, as well as the power to seek information from tech companies and request the blocking of content; (ii) provides users with the right to request the correction or erasure of their personal data; and (iii) allows tech companies to transfer some users' data abroad.

The law also proposes penalties of up to USD 30 million for violations and non-compliance with the law.






The law has been criticized by individuals who believe that the law results in "over-broad surveillance," affects press freedom and dilutes India's right to information law.



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