

Tozzini Freire.

ADVOGADOS

CYBERNEWS.

27th Edition | 2023



Index

01

4

02

10

03

12

04

17

05

18

06

20



Brazilian Context.

ANPD provides clarifications on the role of the Data Protection Officer and the issuance of LGPD compliance stamps

On March 31st, 2023, the Brazilian Data Protection Authority (ANPD) published clarifications to mitigate the spread of misleading information on requirements allegedly made by it.

Among such clarifications, we highlight that ANPD:

- has not yet provided complementary rules on the duties of the Data Protection Officer, which will be subject to future regulation,
- has not officially recognized the enforceability of any rule or guidelines regarding the role of the DPO, and
- does not authorize companies or entities to issue stamps that certify compliance with the Brazilian General Data Protection Law (LGPD).

In addition, ANPD has clarified that the DPO can communicate directly with ANPD and data subjects, with no need for intermediation by any entity. Moreover, there is no legal requirement for data protection professionals or DPOs to be registered before ANPD or any private associations.

New guidelines on the preparation of the Data Protection Impact Assessment are issued by ANPD

In order to provide further clarifications to the public on the preparation of the Data Protection Impact Assessment (DPIA), ANPD published a Q&A document and infographic on the subject, with recommendations on its preparation, the methodologies to be considered by controllers for risk management, and the minimum requirements for it.

Among the many instructions, ANPD recommends that the DPIA be prepared prior to data processing, provides guidelines that should be considered in the risk management analysis, and identifies what can be considered as “high risk” for the purposes of drafting the DPIA.

It is important to highlight that the controller has the legal obligation to prepare the DPIA (art. 5, XVII, and 38, LGPD). Besides, ANPD may request it, for controllers in general, especially with respect to data processing activities involving sensitive data (art. 38, LGPD), and when data processing is based on legitimate interest (art. 10, par. 3, LGPD).

If requested, such document should contain a description of the personal data processing activities that may generate high risk to the application of the general principles of personal data protection set forth in LGPD and to the civil freedoms and fundamental rights of data subjects. In other words, the document should contain at least:

- a description of the categories of personal data processed,
- the methodology used for processing and for ensuring the information security, and
- the controller’s analysis of the measures, safeguards and risk mitigation mechanisms adopted.



Central Bank and credit bureaus sign agreement to share information

The Brazilian Central Bank executed a Technical Cooperation Agreement (ACT) with five database managers, the so-called “credit bureaus,” at the end of March. The ACT aims to enforce the Brazilian Monetary Council Resolution No. 5,037/22, which regulates the access to the Credit Information System (SCR).

The five credit bureaus that have entered into the ACT with the Central Bank are: Boa Vista Serviços S.A., Confederação Nacional de Dirigentes Lojistas (CNDL - SPC Brasil), Gestora de Inteligência de Crédito S.A. (Quod), Serasa S.A., and TransUnion Brasil Sistemas em Informática Ltda.

Both the Central Bank and the companies will benefit from this agreement. On one side, the companies will share data the Central Bank is interested in, such as credit scores and non-banking credit history. On the other hand, the Central Bank may allow the bureaus to access the SCR.

The agreement also included items aimed at protecting the data subjects’ privacy and data, such as preserving the confidentiality of sensitive information and allowing objections to be raised in case of disagreement with any piece of data.



02

Judicial Branch.

Supreme Court of Justice published Data Protection Policy

The Superior Court of Justice Resolution (STJ/GP5/2023) defined its Personal Data Protection Policy, which applies to any data processing operation at the Court.

The policy seeks to ensure the protection of the subjects' information and rights that are under the Superior Court of Justice's responsibility, which must be kept in full and confidentially, as well as processed in accordance with the LGPD and as instructed by control and regulatory bodies.

Under the terms of the Resolution, the presidency of the Court will also create the Personal Data Protection Management Committee, which will evaluate the mechanisms existing at the Court for processing and protecting personal data, as well as encourage new actions and good practices pursuant to the LGPD.

Labor Justice: violation of the LGPD is a reason for dismissal for cause

The judge from the 81st Labor Court of São Paulo acknowledged the dismissal for cause of a nurse who filed a lawsuit against a hospital management company for violating guidelines of the Brazilian General Data Protection Law (LGPD).

The lawsuit sought to acknowledge the constructive termination of the employment contract, so that the plaintiff's dismissal could be converted into dismissal without cause. During the case, however, the employee gathered internal spreadsheets from the hospital with patients' sensitive data.

Consequently, the judge understood that the worker violated the intimacy and privacy of third parties: individuals who were customers of the defendant. Therefore, the judge acknowledged that the plaintiff violated the LGPD, for using sensitive data illegally. In addition, the violation of the LGPD committed by the hospital was also acknowledged, given that the company was responsible for safeguarding its customers' sensitive data.

03

Authorities



Data leakage is included in the ranking of Procon complaints

The report of complaints made in the Procons (Bureaus of Consumer Protection) for the year 2022 brought some news to the internet services sector. For the first time, complaints about application providers were at the top of the list on consumer.gov.br website.

According to the Brazilian Consumer Secretariat (SENACON), complaints about the application providers involved (i) difficulty in contacting someone and delays in the customer service offered by the companies; (ii) problems activating and changing services provided by application providers, and (iii) leakage of personal data and other security incidents.

Although data leakage has not been the most complained about topic in the sector, it is now part of the ranking of complaints for the first time, representing about 15% of consumer complaints.

Although technology companies have been included in the 2022 report, they are also those with the greatest capacity to respond to the problems reported by customers. The resolution rate of consumer complaints reaches almost 83%.

SENACON and ANPD extend Technical Cooperation Agreement

On March 23rd, the Federal Official Gazette published the amendment that extends the Technical Cooperation Agreement between the Brazilian Data Protection Authority (ANPD) and the Brazilian Consumer Secretariat (Senacon), from March 22nd, 2023, to March 21st, 2025.

The main purpose of the agreement is the sharing of collected information involving consumer complaints in the scope of personal data protection. It also provides for joint actions in the areas of consumer protection, including information exchange, standardization of opinions, cooperation in inspection actions, development of education, training and capacity building actions, and the preparation of studies and research. The agreement is part of ANPD's Strategic Planning to promote the development of the Data Protection culture.

With the extension of the agreement, both entities align their efforts and strengthen inspections to ensure that the personal data of Brazilian citizens are protected.

ANPD begins trial of administrative proceedings for Brazilian General Data Protection Law (LGPD) violations

The Brazilian Data Protection Authority (ANPD) has started to assess the first eight administrative proceedings related to alleged violations of the Brazilian General Data Protection Law (LGPD). Most cases involve federal public sector agencies and personal data leaks.

The regulation on the measurement and calculation of penalties published by ANPD allows the authority to punish public and private sector agents for violating the LGPD, with fines of up to BRL 50 million.

In addition to sanctions, ANPD may require the adoption of corrective measures to prevent further violations affecting data subjects. According ANPD's director, a second group of lawsuits involves private companies, with situations that go beyond security incidents, such as selling and sharing data.

ANPD will concentrate its efforts on the largest data processing agents. Digital platforms, social media, e-commerce, telecommunications, and the public sector will be the main targets of inspection at this first moment.

For ANPD, the goal is more than punishing violators; it is rather to draw attention to the need to comply with the law and ensure the safety and protection of citizens.

Prosecution Office.

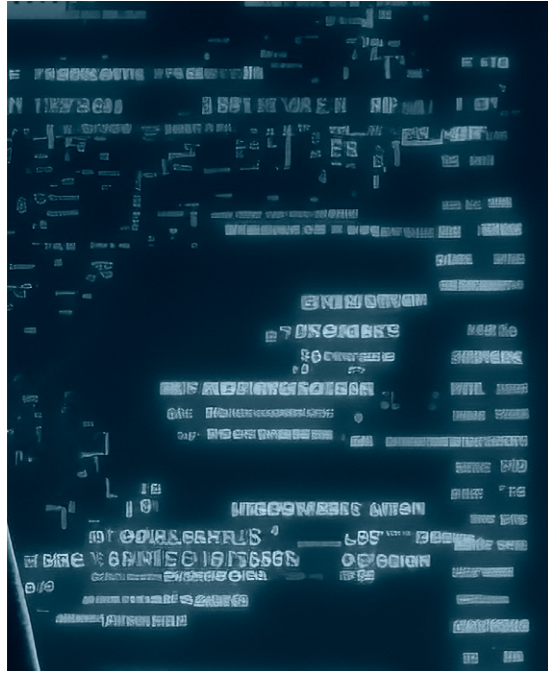
021

Federal Prosecution Office publishes report on personal data protection activities

Faced with the new challenges posed by the Brazilian General Data Protection (LGPD), the Federal Prosecution's Office established a specialized sector to deal with issues related to personal data and created the Personal Data Protection Unit (UPDP). The Unit is linked to the Federal Attorney General's Office and works with the Data Protection Officer on activities related to the informational self-determination of personal data subjects.

With the 2022 Activity Report, the Unit aims to account for the activities and promote transparency of the actions taken by the institution and the results achieved.

The action plan has already been made, delimiting the different fields of work, which are Governance, Compliance, Transparency, Contracts and Data Security. The plan also includes the activities expected for each field of work, for the period from June 2022 to June 2023, as well as information on meetings and events.



05

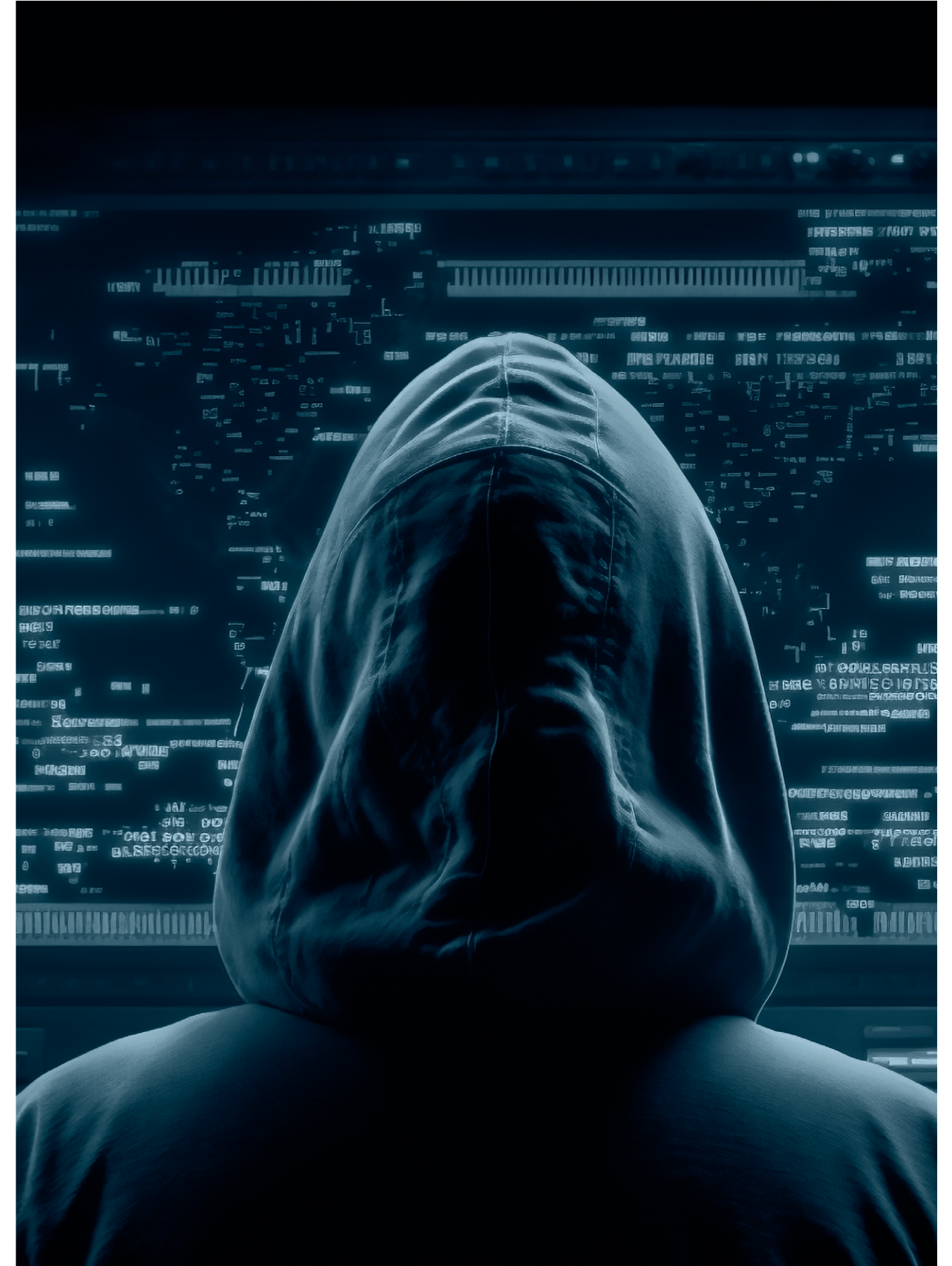
Normative Developments.

The Convention on Cybercrime is enacted

On April 13th, 2001, the [Convention on Cybercrime](#) was enacted. The Convention was signed by Brazilian representatives in Budapest, Hungary, on November 23rd, 2001. Currently, 66 nations are signatories to the Convention, which aims to foster international cooperation for combating crimes committed through internet.

The Convention's assumptions include preventing actions against confidentiality, integrity and availability of computer data, systems and networks, as well as preventing any misuse of these systems. It also describes several cybercrimes, such as illegal access, data breach, system interference, and crimes related to the shared information.

After this enactment, Brazilian authorities will be able to more easily investigate crimes carried out in the digital environment, especially those which involve evidence obtained abroad and, likewise, Brazil undertakes to assist foreign authorities that are signatories to the Convention.



06

International Rulings.

European Data Protection Board publishes new version of its guidelines

On March 28th, 2023, the European Data Protection Board (“EDPB”) published the second version of its [“Guidelines 9/2022 on personal data breach notification under General Data Protection Regulation – GDPR.”](#)

The guidelines set forth standards to determine the risk level of a given incident that the controller has identified or became aware of. These standards are helpful within the EEA for clarifying whether a security incident should be reported to the data protection authorities or to the affected data subjects.

In this context, the EDPB acknowledges that the assessment of the “risk to the rights and freedoms of data subjects” should consider criteria such as:

- the type of breach,
- the nature, volume, and sensitivity of the affected data,
- how easy it is to identify the data subjects whose data were involved in the breach,
- the concrete consequences (such as the potential to cause identity theft, physical harm, psychological distress, humiliation, or reputational damage),
- the potential vulnerability of the data subject,
- the degree of risk of the activity carried out by the data processor, and
- the number of affected data subjects.

With these standards in perspective, if the potential risk to data subjects is identified, the European data protection authorities should be notified (as well as the data subjects if the risk in question is high). Also, the guidelines clarify that data processors must report the incident to the authority of each country in the EEA where affected data subjects have been identified.

ChatGPT is temporarily banned in Italy and investigated by Canadian Authority

The text generation platform via AI has been temporarily banned from operating in Italy and has also become the subject of an investigation in Canada, between late March and early April. The data protection authorities from those countries are concerned that personal data may be processed without proper consent.

In addition to the temporary ban, the Italian authority said it is preparing an investigation to check whether OpenAI, the company that owns ChatGPT, operates in compliance with the GDPR. The Canadian authority, however, did not reveal further details about the ongoing investigation.

Moreover, the Italian authority has set a deadline for OpenAI to explain how the issues raised by the authority will be addressed. If the deadline is not met, fines of up to EUR 20 million or up to 4% of the company's annual revenue could be imposed.

On April 13th, 2023, during a meeting of the EDPB, it was decided that a joint task force will be established to discuss issues involving data protection and ChatGPT.



487095484

265873282

```
age = ATOMIC_INIT(2) );  
dsetsize){
```






```
struct group_info init_groups = { .usage = ATOMIC_INIT(2) };  
struct group_info *groups_alloc(int gidsetsize){  
struct group_info *group_info;  
last one indirect block pointer */(int nblocks)
```

376984373

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

821439828

```
struct group_info init_groups = { .usage = ATOMIC_INIT(2) };  
struct group_info *groups_alloc(int gidsetsize){
```