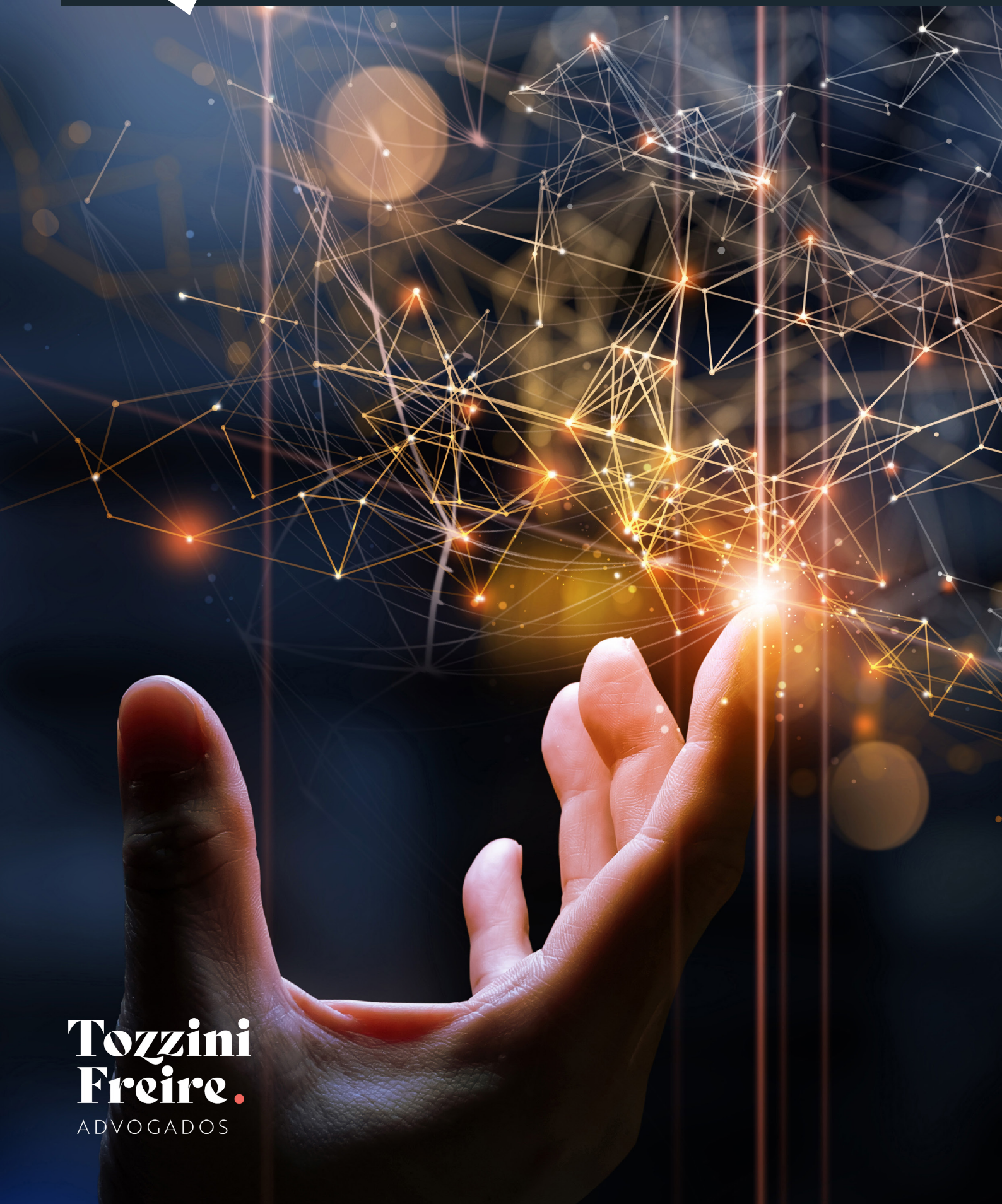
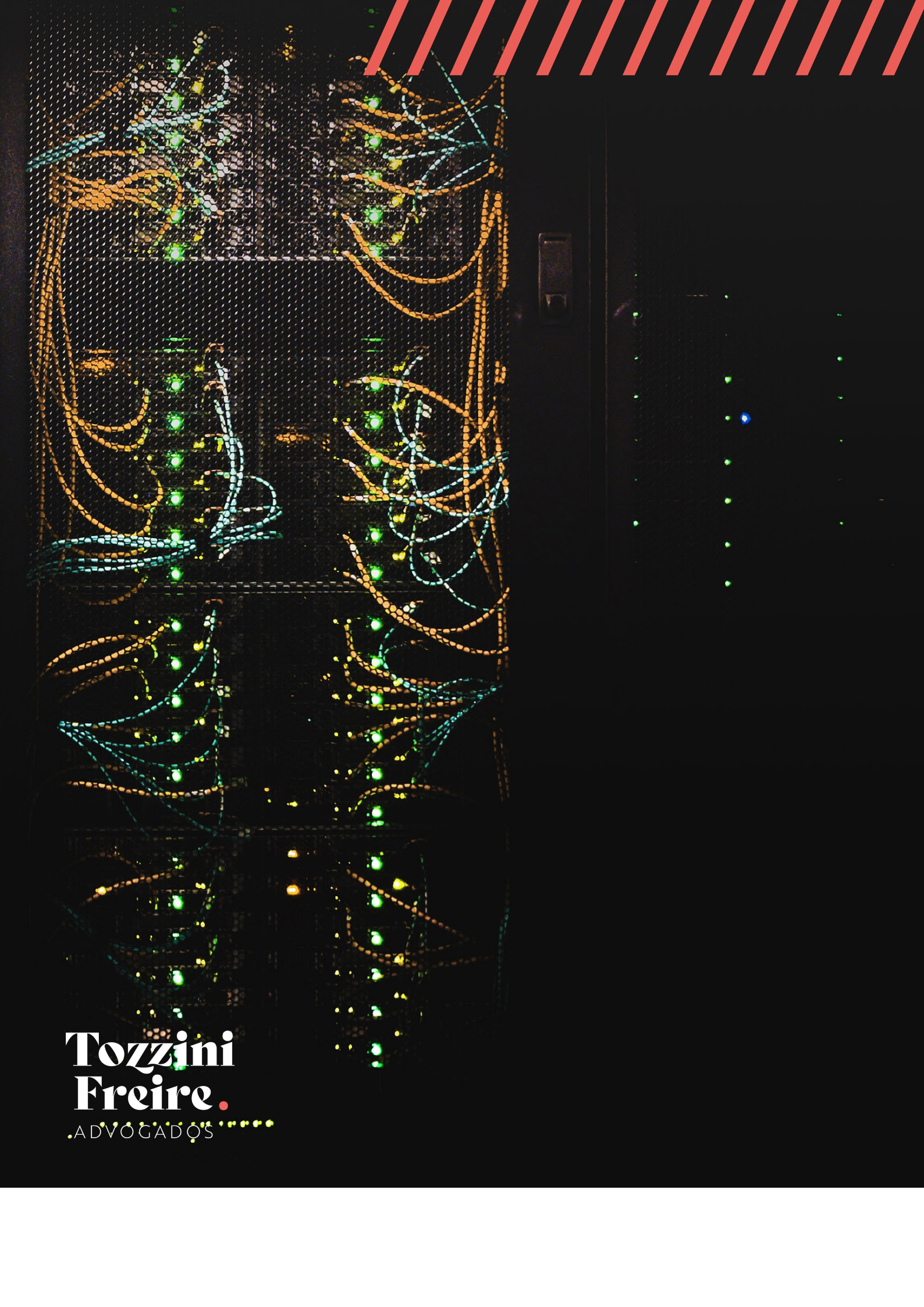
21st Edition | 2022

cybernews.



Tozzini Freire.
ADVOGADOS



Tozzini Freire.
ADVOGADOS

index

///// Brazilian Context

The Brazilian Senate approved the Provisional Measure that transforms the ANPD into an autarchy of a special nature

On October 18, 2022, the Federal Senate approved the Provisional Measure No. 1,124/2022, which transforms the National Data Protection Authority (ANPD) into a special agency.

The update of ANPD's legal nature was already set forth in the Brazilian General Data Protection Law (LGPD), which provided that it could be transformed by the Executive Branch into an indirect federal public administration entity, subject to a special autonomous regime and linked to the Presidency of the Republic.

With the approval of the Senate, the document will be forwarded for publication in the Official Gazette.

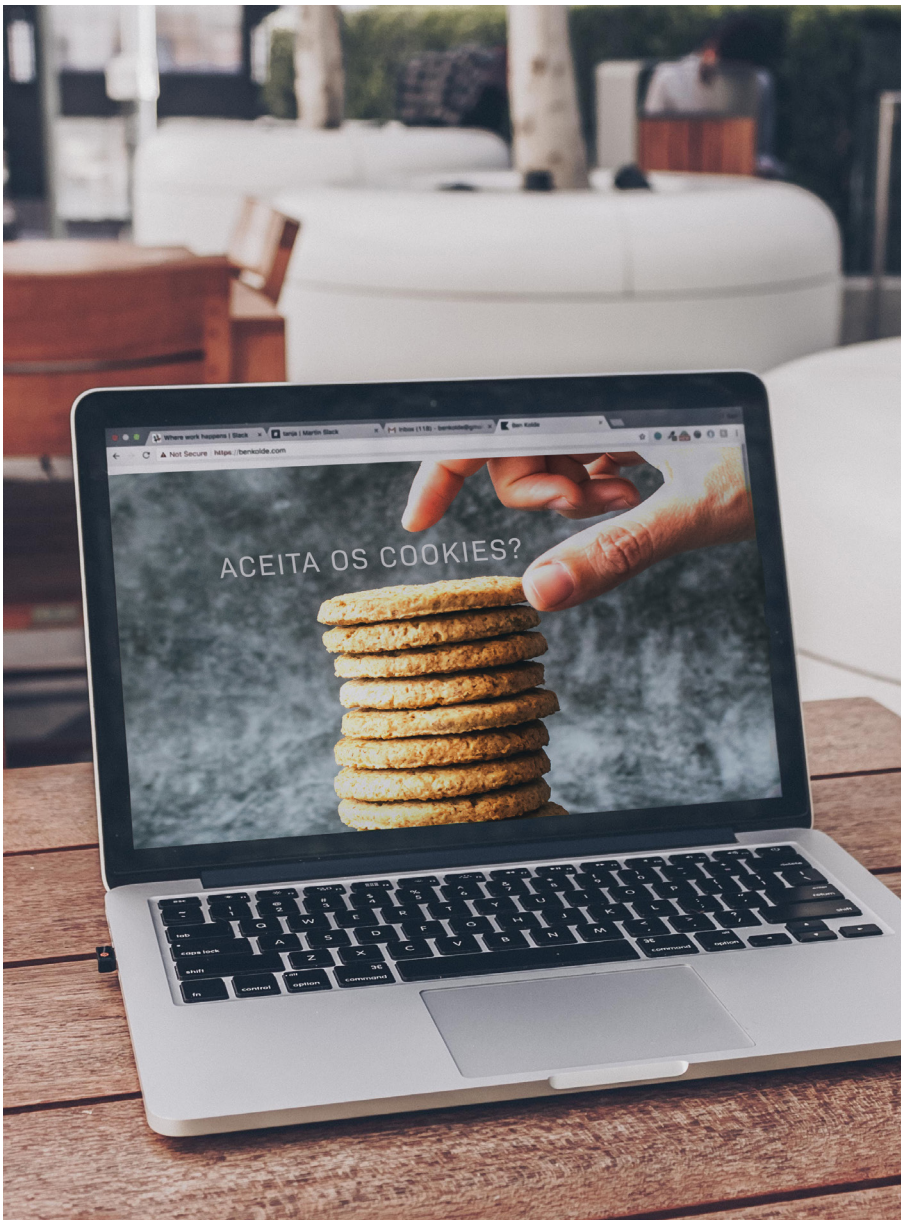
ANPD publishes guidelines on "Cookies and Personal Data Protection"

On October 18, 2022, the ANPD published the guidelines on "Cookies and Personal Data Protection".

Despite not being a binding document, the guide aims to guide processing agents on good practices involving the topic, in addition to providing an overview of the subject.

In a nutshell, the ANPD:

- Recognizes the existence of other legal hypotheses, in addition to consent and legitimate interest, for the collection of personal data through cookies (p. 17);
- Advises against the use of cookie banners with pre-selected options ("on by default"), requiring an active conduct by the data subject in this regard – exception made to necessary cookies (p. 19); and
- Advises consent for unnecessary cookies (i.e. cookies whose disabling does not prevent the website or application from functioning or the user's use of services) (p. 20).



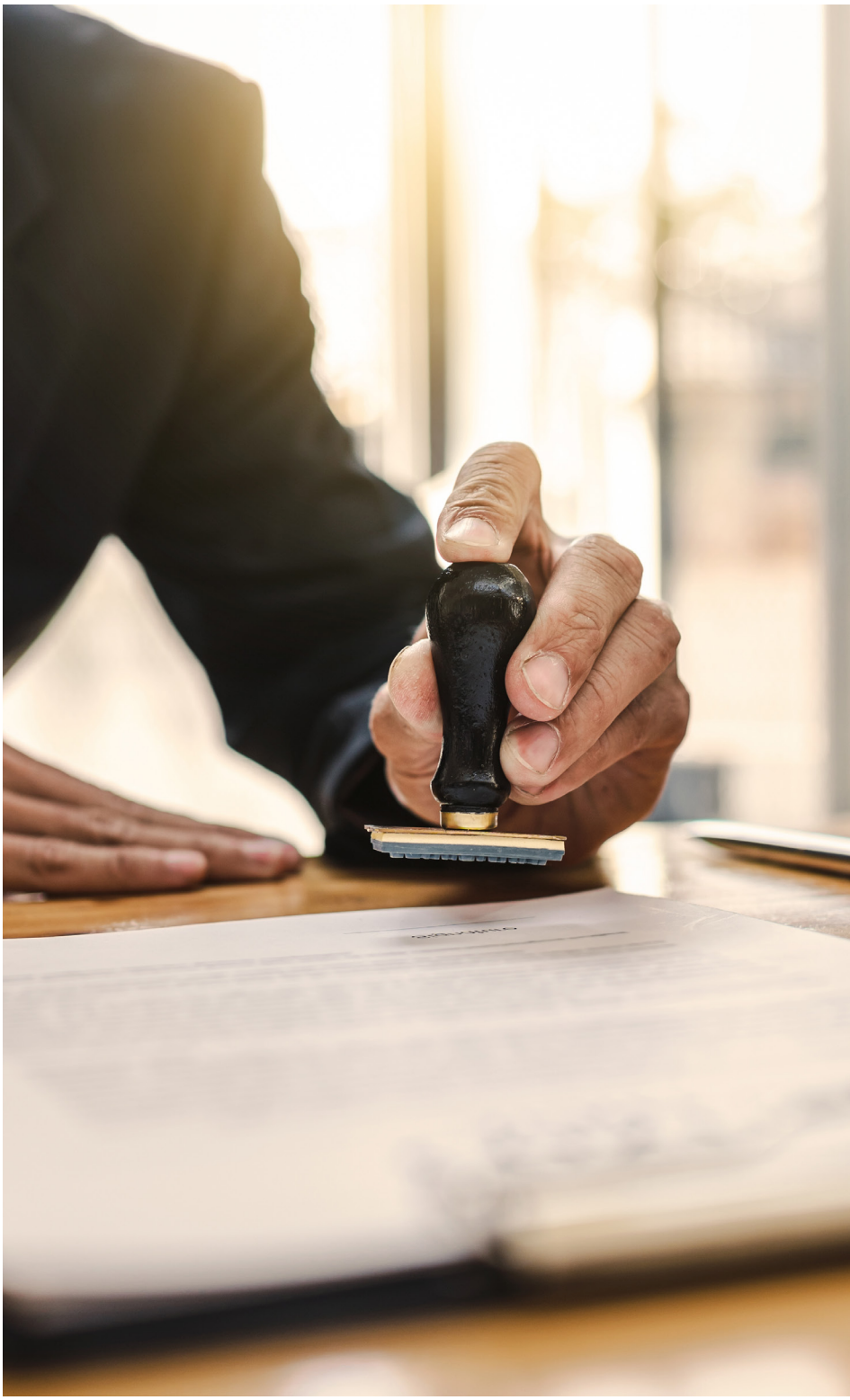
In the ANPD's perspective, legitimate interest may be the most appropriate legal hypothesis for collecting data through necessary cookies, since these cookies are used to support and promote the activities of the controller and to provide the services that benefit the data subject; as well as for analytical cookies, in certain contexts (p. 24).

ANPD also reinforces the importance of providing transparent information to the data subject. This can be provided in a Cookie Policy (that may be a section of the Privacy Notice itself), or diluted in a cookie banner (p. 28 and 29).

The guide will be open to ongoing comments and contributions from society. The objective is that the material is always updated, whenever new regulations and understandings are established. Suggestions can be sent to the ANPD Ombudsman, through the Fala.BR Platform.

The complete version of the guide can be consulted here (available in Portuguese).

Registry Offices must adapt to new data protection rules by March 2023



At the end of August, the National Council of Justice (CNJ) published Provision No. 134/2022, which regulated the process of adaptation of extrajudicial registries to the Brazilian General Data Protection Law (LGPD). The CNJ's expectation with the publication of the Provision is to adopt more transparent procedures in the scope of personal data processing activities.

Among the provisions of Provision No. 134, there is the mapping of the processing activities – which will identify the processing activities to be carried out, the personal data processed, their purpose, and the expected duration of the processing – and the annual maintenance of the information inventory. It should be noted that, in addition to the above topics, the Provision encourages the elaboration of effective procedures for dealing with the data subject's rights.

In this sense, it is worth noting that the Provision is directly related to the nature and volume of personal data handled by the extrajudicial registries, connected to issues such as filiation, death, birth, and several patrimonial legal relations, on a considerably high volume.

Moreover, it also sets forth that such inventory of data must be filed in the notaries' offices and made available should the CNJ request it, through the Inspector General's Office, the Brazilian National Data Protection Authority (ANPD), or other supervisory bodies.

Federal Council of Medicine (CFM) publishes a guidebook for doctors on the application of the LGPD

To promote greater security in the processing of personal data in the healthcare field, the Federal Council of Medicine (CFM) has published a guidebook on personal data protection for physicians. Health organizations should aim to be in full compliance with the Brazilian General Data Protection Law (LGPD) since they deal with health data, which are sensitive personal data and, therefore, should be preceded by special precautions in their processing.

The guidebook provides the main definitions set forth in the LGPD and the instructions on the necessary steps to be taken by physicians to ensure the effective confidentiality of personal data, and it also outlines the roles of data processing agents, with a full focus on healthcare.

Special attention should be given to the processing of personal data related to health, which must be done with the consent of data subject, but the guidebook highlights some exceptional cases that may take place without the collection of consent, such as the maintenance of the patient's medical record, to meet standards that provide for the safekeeping of the document for public utility purposes.

CNseg launches new service for reporting cyber incidents

In September, the National Confederation of Insurers (CNseg) adopted the so-called Sharing of Cyber Incidents (CIC), which consists of a system to centralize the reporting of cyber incidents to all supervised companies.

This new service allows insurance companies to reduce operational costs to comply with the requirements of the SUSEP Circular No. 638/2021 – for the alignment of the insurance market with the provisions of the Brazilian General Data Protection Law (LGPD) – because their security incidents may be reported to several supervised companies simultaneously and also because initiatives to protect the damage caused by the incidents will be carried out more quickly.

Furthermore, the companies joining the CIC will have exclusive access to solutions that can increase revenue, optimize and improve the pricing, quotation, subscription, and claims-regulation processes, reduce costs, mitigate risks, prevent and combat fraud, and maintain legal compliance, resulting in continuous improvement in the provision of services to clients.

ANPD publishes Technical Note analyzing the Cooperation Agreement between SERPRO and a company

On September 21, 2022, the ANPD published Technical Note No. 75/2022/CGF/ANPD, which analyzes the possible sharing of personal data under the Agreement of Technical cooperation between the Federal Data Processing Service (SERPRO) and DrumWave. DrumWave is a company that carries out activities similar to a digital data registry, monetizing the value of the data of companies and people.

In this sense, given that there is currently no sharing of personal data in the context of such Agreement, no action of the ANPD is necessary at this time. However, should SERPRO, at a future moment, choose to share personal data within the scope of the Agreement, it must notify the Authority immediately.

AEPD & EDPS publish joint paper on misunderstandings about Machine Learning

On September 20, the Spanish Data Protection Authority (AEPD) and the European Data Protection Supervisor (EDPS) published a joint paper commenting on several popular misconceptions related to Machine Learning (ML). The publication, available on the EDPS website, aims to dispel misconceptions about systems using ML while highlighting the importance of using such systems in accordance to data protection principles.

Among the myths addressed are sayings such as "ML systems are less subject to human biases"; "ML can accurately predict the future"; and even "Automatic decisions taken by ML algorithms cannot be explained".

In several of these myths, the root cause usually relates to the mistaken belief that ML would be free from human interference, which is far from reality. Most ML systems today rely on humans for initial and usual selection, cataloging, design, and training of the data; at all of these stages, the ML system would be subject to human biases.

In this sense, the growing concern about automated data processing, as well as about potentially biased decisions made by ML systems, is justifiable; hence the attention of data protection legislations and authorities to the topic.

ICO/UK publishes guidance on privacy enhancing technologies

In September 2022, the Information Commissioner's Office (ICO) – the UK's independent authority responsible for upholding the public interest in data privacy matters – published a guide on privacy enhancing technologies (PETs) (access here).

PETs allow organizations to process personal data in a responsible, secure, legal, and collaborative manner by, for example, reducing the degree of identity of the individuals to whom the data is processed, minimizing the amount of data processed, anonymizing the data, and splitting or controlling access to personal data.

Although PETs are already used by financial organizations in money laundering investigations and by the health sector in providing better health services to the public, the use of PETs is still in its early stages. For this reason, the guidelines encourage the use of PETs, demonstrate the different types that exist, and explain the benefits of their use for compliance with data protection laws.

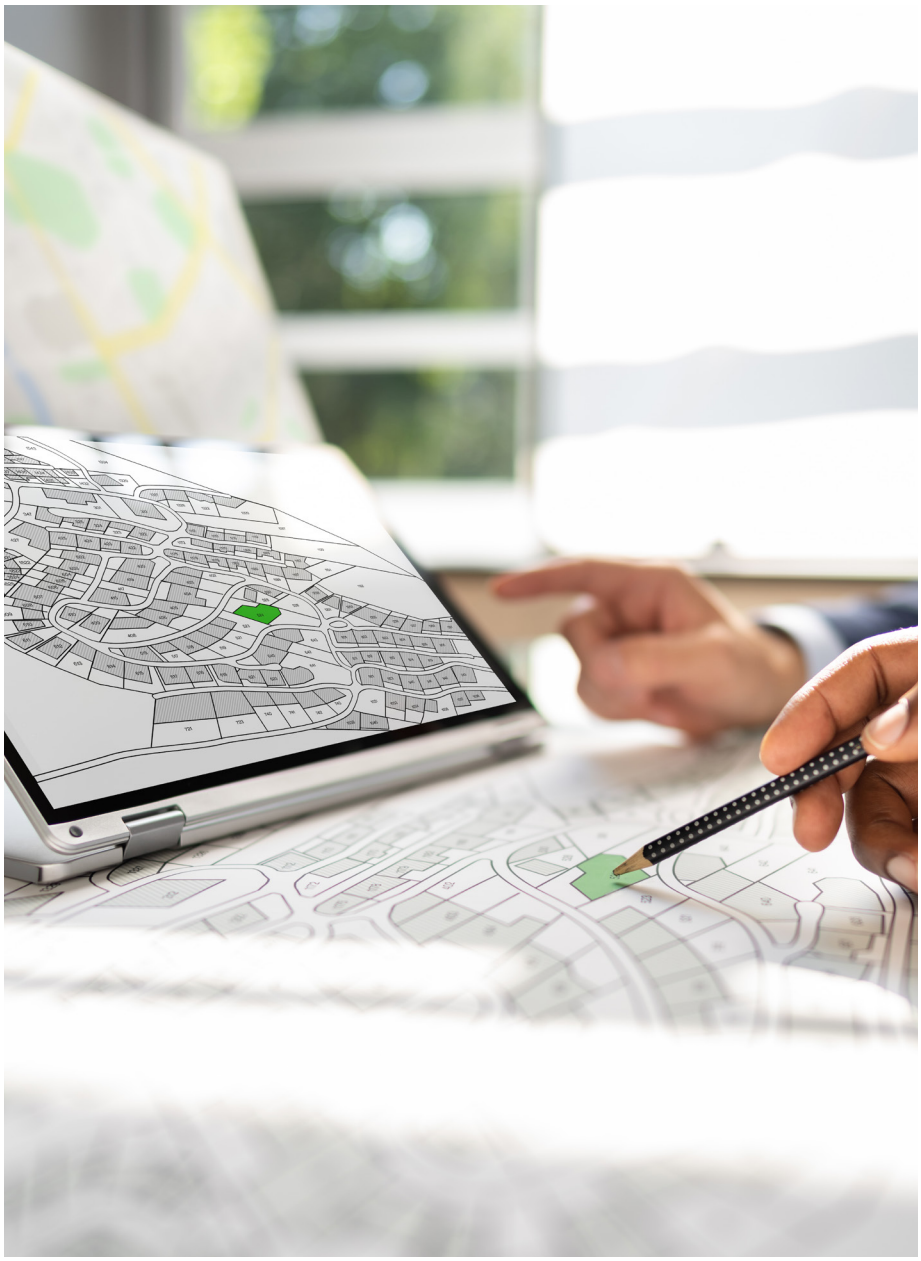
ICO/UK publishes personal data sharing guide for university students

On September 14, 2021, the ICO published a Guidance Guide for universities and students about the necessary care and good practices to be followed in the sharing of personal data.

Among the practices indicated is the preparation of a Data Protection Impact Assessment, to identify in advance potential failures in the security of data sharing and assist in the planning of emergency procedures to be followed in case of incidents. In addition, another recommendation is to implement the execution of Data Sharing Agreements between those involved (university and students), so that information is shared in a safe and legitimate way.

Finally, another recommended practice is to train university employees about their responsibilities, the rights of the data subjects and the principles that must be followed when processing and sharing personal data.

G7 data protection and privacy authorities discuss data protection and the flow of data across borders



Data protection authorities from the G7 countries met in Bonn, Germany, in early September, to develop joint strategies linked to the concept of "Free Flow of Data with Trust". The meeting is the second of its kind, demonstrating keen interest of the global economies in adopting global best practices for data protection.

In general terms, the meeting's guiding principle is to build consumer trust by ensuring global data protection standards for the international flow of data.

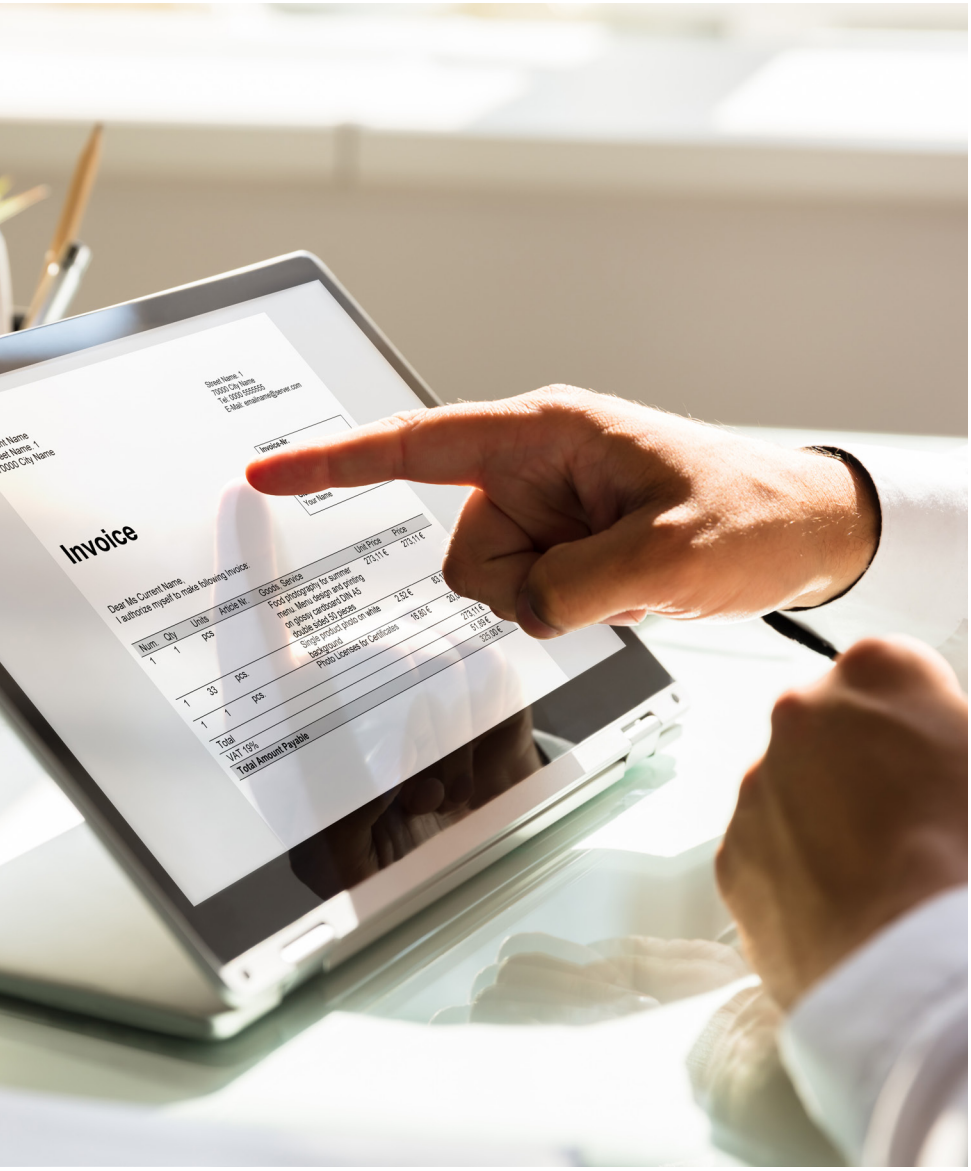
Among the discussions that received input from authorities is the creation and maintenance of "international data spaces," seen as an emerging approach for sharing national or international data, in a trusted and voluntary way, within organizations and sectors to support innovation in academia, industry, and public administration.

Germany's BSI publishes report on tech in automotive industry

On September 19, 2022, the German Federal Office for Information Security (BSI) published the second edition of the Automotive Sector Situation Report 2021/2022, which analyzes cybersecurity in the automotive sector, both in terms of respect to the industry, as to the vehicles themselves.

In this sense, in view of the rapid technological progression in the automotive sector, as well as the advancement of potential threats from various types of cyberattacks, the document provides an overview of the contemporary scenario of the digitization of the automotive sector in Germany in order to increase cyber security in the country. Thus, the Report provides care tips and recommendations that the industry should keep in mind when developing products, as well as covering vulnerability management and other aspects focused on automation and artificial intelligence security.

In the terms of a statement granted by BSI President, the Report "highlights once again that cybersecurity must be considered at all links in the supply chain – from the beginning to the finished product." It is therefore of paramount importance that the new technologies needed to ensure proper security are not manipulable and that possible cyberattacks have no impact on the safety of driving motor vehicles.



CNJ adheres to LGPD in the digitalization of law suits

The National Council of Justice (CNJ) approved, in October, Resolution No. 469/2022, in order to establish new standards and guidelines for the digitization of judicial and administrative documents and for the management of documents in already digitized processes, with the exception of the Supreme Court (STF).

Incorporating the Brazilian General Data Protection Law (LGPD), the Resolution has, among its purposes, to ensure and preserve the integrity, authenticity, confidentiality, and preservation of judicial and administrative documents.

The text of the Resolution details document management policies, seeking that Public Agencies adapt to the LGPD and manage to preserve and guarantee the quality of judicial and administrative files. In this way, judicial entities should promote the distinction between documents that should be discarded and those that should be preserved, accessed and disseminated, becoming part of the Brazilian Judiciary's heritage.

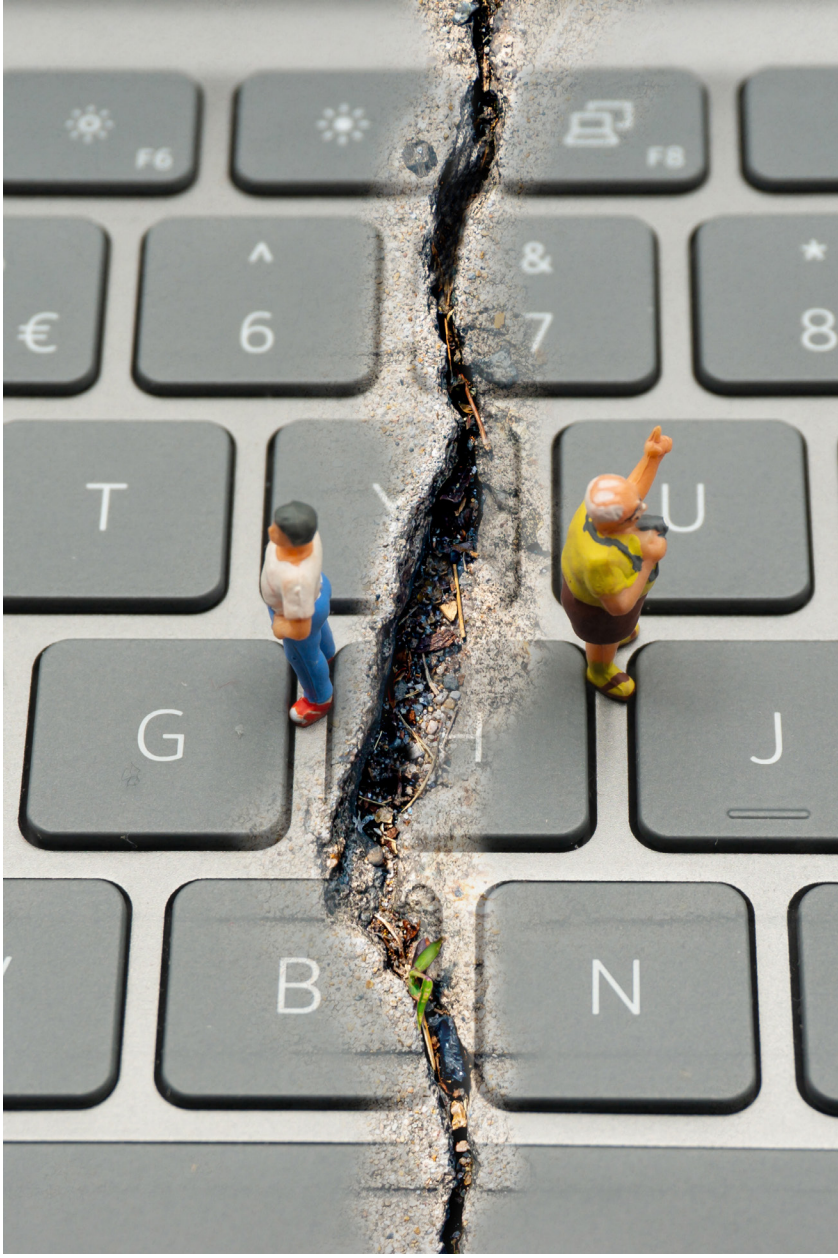
Salise Monteiro Sanchotene, president of CNJ's Permanent Commission of Document Management and Memory of the Judiciary, brought important data regarding the digitalization of judicial processes in Brazil. Highlighting the large growth in the percentage of exclusively electronic new cases, which reached 96.6% in 2020, she also emphasized that there is still a considerable amount of physical cases that are to be digitized.

The Supreme Court rules on the principles and guarantees protecting personal data must be observed by public entities when sharing data

The judgment concerning the use of the parameters established by the General Personal Data Protection Law in the rules of Decree No. 10,046/2019 ended on September 15. Such decree deals with the sharing of personal data between federal agencies that regulates data sharing within the federal public administration and establishes the Citizen's Base Register, as well as the Central Data Governance Committee.The Federal Supreme Court decided, by majority vote, that the Decree that created the Citizen's Base Register – which gathers information about citizens from different public administration bodies – should be interpreted in accordance with the Constitution, following a series of principles that were established by the Rapporteur Gilmar Mendes.

Among the principles are that data sharing must be limited to serving the informed purpose and that the guarantees and procedures established in the General Law of Data Protection must be met with regard to the public sector.

TSE creates intelligence group to combat political violence



After a meeting between the current President of the TSE (Brazilian Superior Electoral Court), Minister Alexandre de Moraes, with the general commanders of the military police, on July 24, to discuss the security of the elections, they decided to establish an intelligence nucleus to combat violence in the elections.

The nucleus was created in early September, through the publication of Ordinance TSE No. 833, with the objective of collecting and processing public security data during the electoral period to combat political violence.

The group will be formed by Minister Alexandre de Moraes, and other members of the TSE, such as Auxiliary Judge Marco Antonio Martin Vargas, who will be responsible for the Executive Secretariat. On the part of the CNCG (National Council of Commanders-General of the Military Police), some lieutenant colonels will integrate the group. Members will work together throughout the election period to prevent and identify cases of political violence.

TSE Ordinance No. 833 does not expressly establish how this will be done, but only states that it will be defined by the President of the Court, Minister Alexandre de Moraes, at the first meeting of its members.

TJMG understands that the dataroutinely provided is not sensitive data

The 18th Civil Chamber of the Court of Appeals of the State of Minas Gerais (TJMG) dismissed the appeal filed by a consumer who sought to amend a judgement so that the defendant Banco FICSA was ordered to pay moral damages for alleged violations of the Brazilian General Data Protection Law (LGPD).

The Appellant had filed the action against the bank for, in addition to the mentioned compensation, obtain double payment of the amount charged for a consigned loan not contracted, and the sentence was upheld only in relation to the double refund of the amount.

Although it was uncontroversial the hiring of a payroll loan without consent of the Appellant, the Court held that the consumer has not proven the requirements for compensation for moral damages. As main grounds, the Court noted that the LGPD provides that only the use of data characterized as “sensitive” may give rise to compensation. However, according to the Court, personal data is not considered “sensitive” when it can be accessed by third parties, and is routinely provided in commercial establishments or mobile applications.

In addition, the Court also understood that the causal link between the alleged data leak and the loan contracting was not proven.

Despite the Court’s understanding, we emphasize that it is contrary to the proper interpretation of the law, since there is no provision in the LGPD that limits civil liability for violation of the personal data protection law only when it involves sensitive data.

Minas Gerais State Court of Appeals denies unrestricted access to public records in the Court's partner systems

In the original lawsuit, the plaintiff requested the lower court the adoption of measures to obtain personal data from the defendants in order to locate the heirs of the owners (already deceased) of the real estate that is the object of the claim of ownership.

Besides the commonly granted requests (such as diligences in front of "SISBajud, Renajud, Infojud"), the plaintiff also requested access to personal databases offends the constitutional protection of privacy, acknowledges the Minas Gerais State Court of Appeals. The appellant had requested unrestricted access to information in public registers in the systems of the Court in order to identify and locate the heirs to be part of the passive pole of the original lawsuit, but the 21st Specialized Civil Chamber understood by the need for prior minimum individuation of the people to whom the research is intended to be made.

According to the Court, the claim of unrestricted access to personal databases offends the Brazilian General Data Protection Law, in addition to the constitutional postulate of privacy protection, considering the lack of a demonstration of the legitimate and proportionate purpose of such processing of personal data. As the ruling explains, "Personal data may be publicly accessible but may not be generally captured for any other purpose by third parties."Thus, it was the burden of the interested party to indicate the specific indication of the persons whose personal data is sought in the systems contracted to the judiciary, in order to analyze the purpose and context of the request for obtaining personal data.

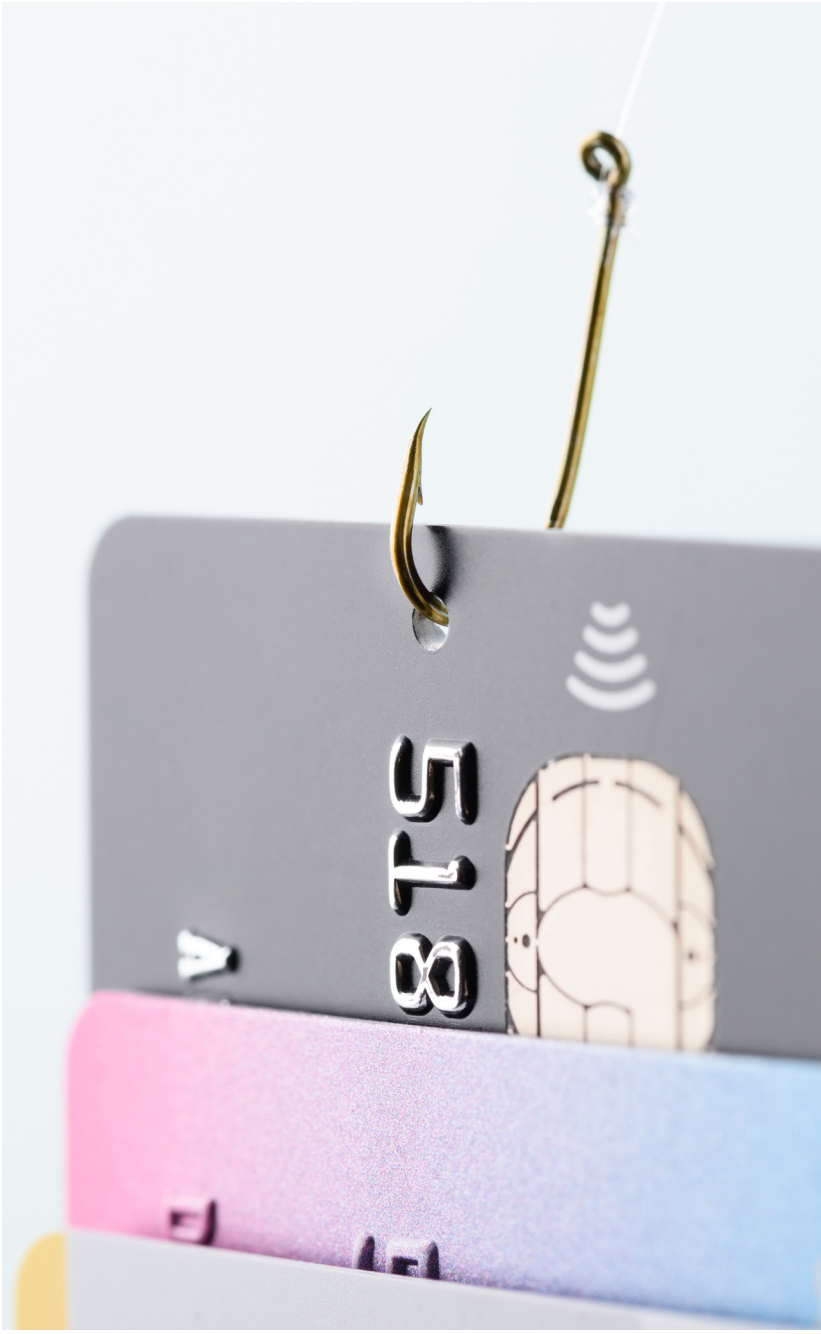
São Paulo State Court of Appeals upholds the legality of disclosing non-sensitive personal data related to credit protection activities

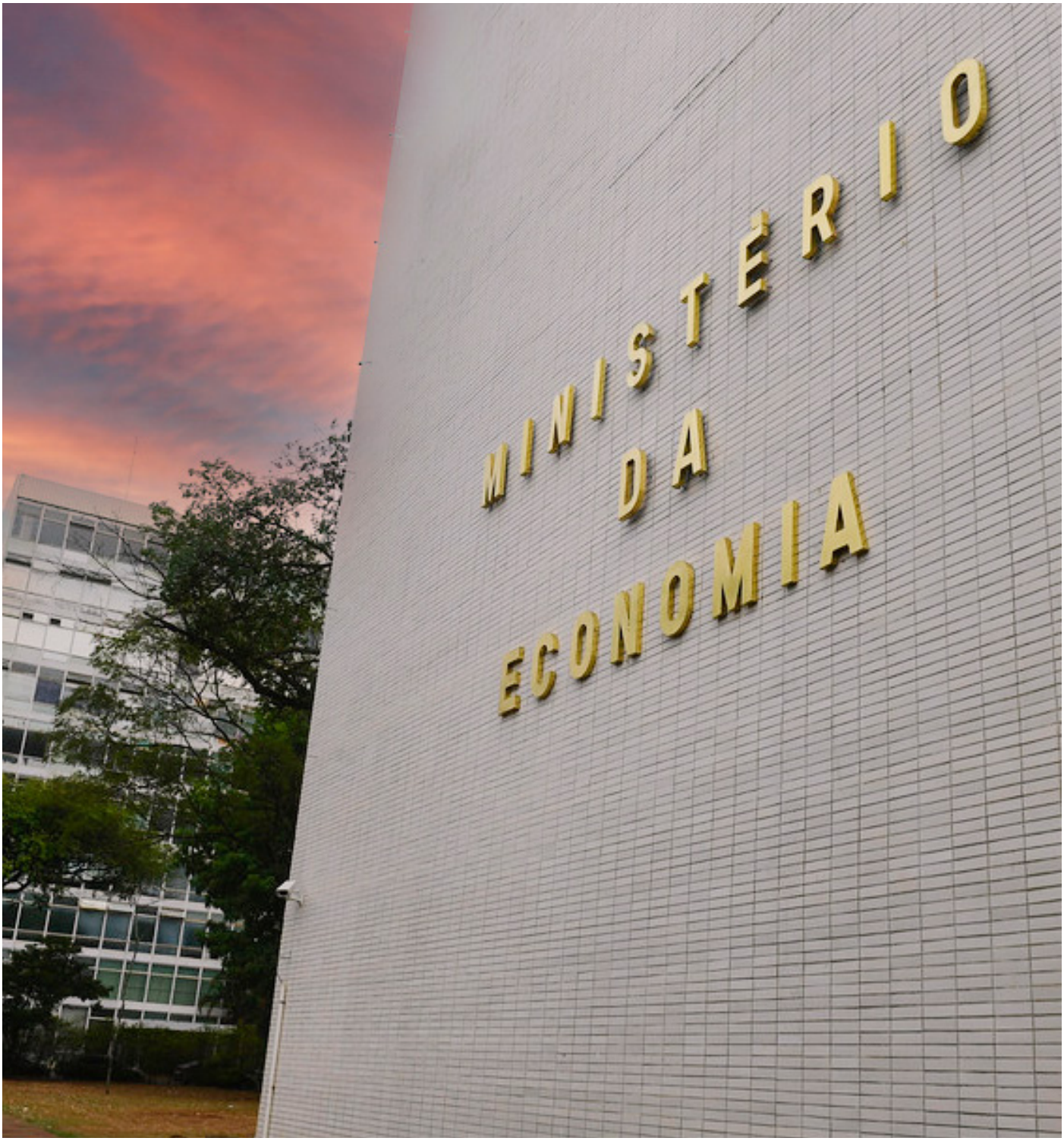
São Paulo State Court of Appeals upholds the judgment that established that registration data, not being sensitive data, does not require authorization or communication from their owner or prior communication for its disclosure by company operating in the field of credit protection relations.

In the original lawsuit, the Plaintiff requested that Serasa S/A be ordered to refrain from disclosing his data (such as "*monthly income, address and personal telephone numbers*") and to pay damages due to the alleged lack of authorization for the commercialization of his personal data. The Plaintiff claims that it would be unacceptable for the company to make available in a database information about which no prior notice had been given.

The Court upholds the judgment that denied the Plaintiff's requests and considered that there was no proof by the Plaintiff that there had been alleged improper disclosure of his data, and, furthermore, that the information disclosed and discussed in the records is necessary to support the credit analysis.

The precedent confirms the position of the 2nd Chamber of Private Law – already exposed in other cases – regarding the legality of data disclosure in the context of subsidizing credit analysis by companies operating in the sector.





MPF opens inquiry about sharing of citizens' data by the Ministry of Economy

The Brazilian Federal Public Ministry has opened a civil investigation to investigate the cooperation agreement signed between the Ministry of Economy, the Federation of Brazilian Banks and the Brazilian Association of Banks, which authorized more than 100 financial institutions to access biometric and personal data of citizens stored in the national database of citizenship (called "*National Civil Identification*") and the Gov.br platform for a period of one year, for purposes of digital identity.

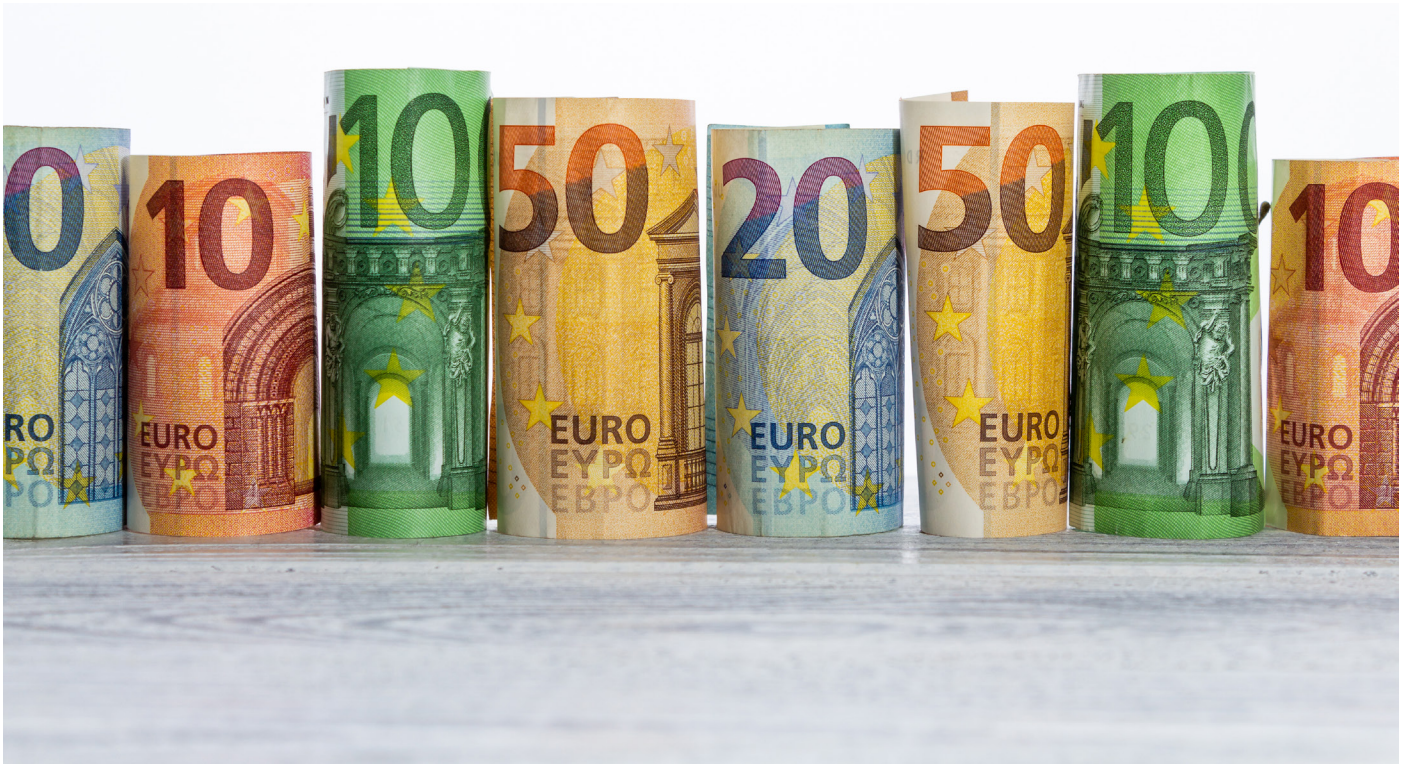
The Ministry of Economy has said to the press that, until the present moment, the acts were reviewed by the Brazilian National Data Protection Authority (ANPD) and the Brazilian Court of Accounts (TCU), which ruled for their legality and filed the cases.

Berlin DPA imposes 525K euro fine over DPO violation

On September 22, the Berlin Authority for Data Protection and Freedom of Information convicted a retailer located in the city of Berlin, Germany, for failing to comply with the requirements related to the In Charge present in the European General Data Protection Regulation (GDPR).

The Berlin authority's decision came, however, after a first warning to the retailer was issued in 2021. In addition to the first guidance, the Berlin data protection authority conducted an investigation that led to its conviction of the potential infringement of article 38 (6) of the GDPR. The said article deals with the tasks and duties to which the DPO may be subjected by the controller or operator, requiring that these tasks do not result in a conflict of interest.

The fine, however, as per the report of the Berlin data protection authority, is not yet judicially binding, so the DPO may still plead for its annulment.

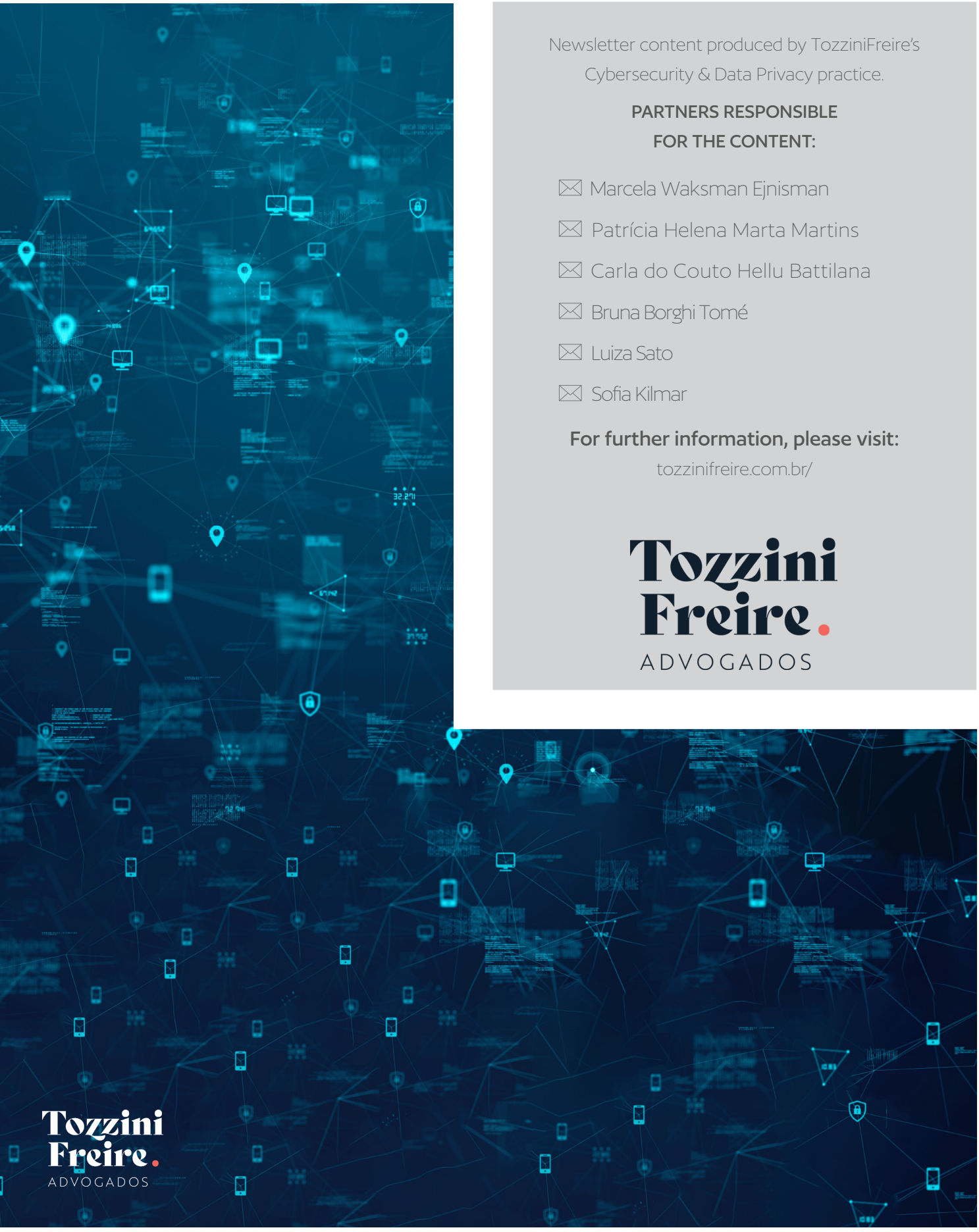


EDPS responds to the violation of the New Europol Regulation

On September 16, 2022, the EDPS – the data protection supervisory authority of EU institutions, bodies, offices and agencies – requested the Court of Justice of the European Union (CJEU) to declare the annulment of two provisions of the new European Union Agency for Law Enforcement Cooperation (Europol) Regulation, which has been in force since June 28, 2022, because they impact personal data processing activities carried out by Europol in the past.

These two provisions (Articles 74a and 74b of the Regulation) retroactively legalize Europol's practice of processing large volumes of personal data that had been transmitted to Europol to verify whether the individual has any established connection with criminal activity. If such connection was not verified, these personal data must be deleted no later than January 4, 2023, as instructed by the EDPS. The new provisions of the Europol regulation allow Europol to continue processing data that has not yet been deleted, despite the EDPS' order.

For this reason, these provisions threaten both the legal security of individuals' personal data and the independence of the EDPS.



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

Imagens: Shutterstock, Taylor Vick, Ben Kolde, Tijana Drndarski, Marcos Oliveira/Agência Senado