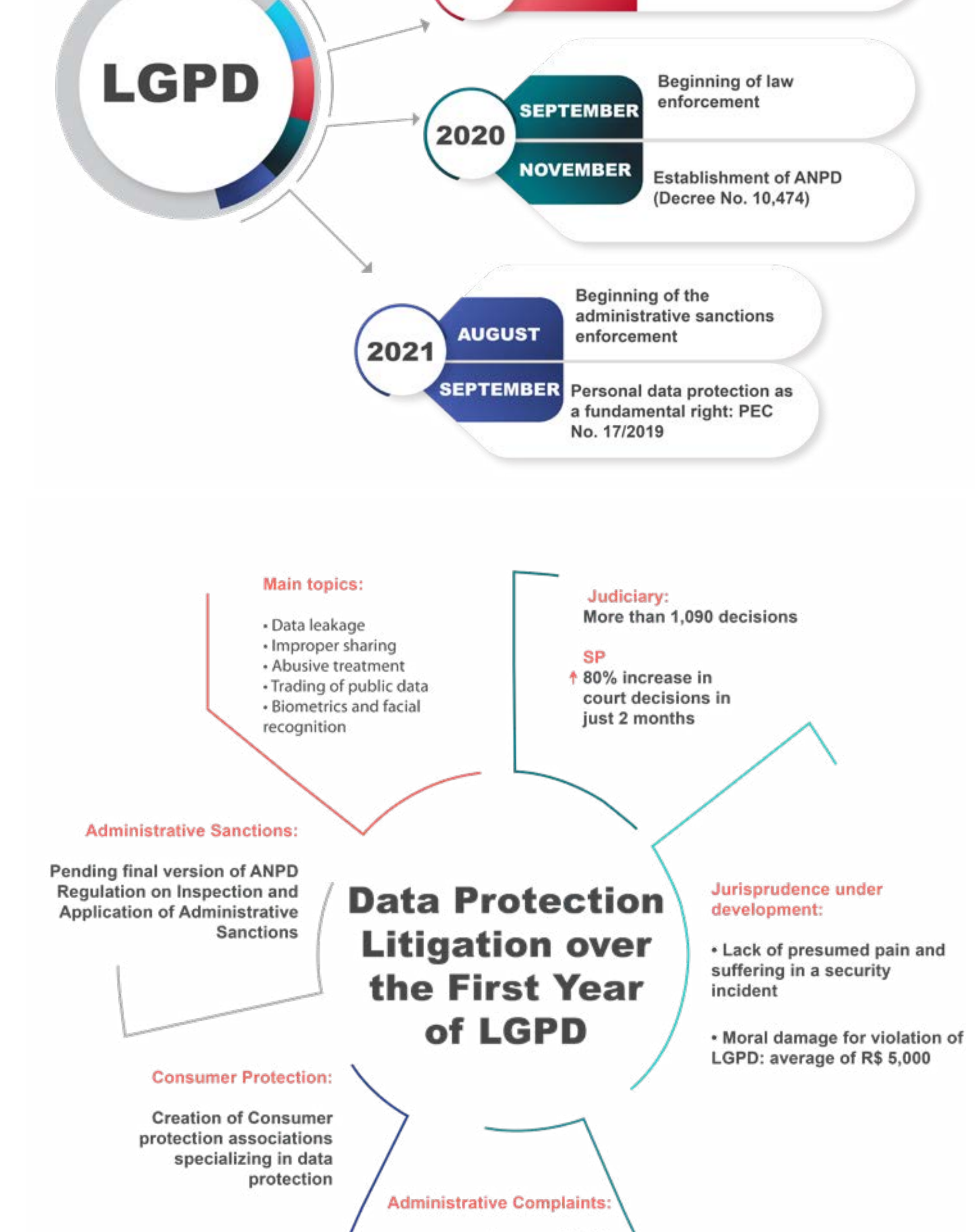


SPECIAL EDITION: 1 YEAR OF ENFORCEMENT OF LGPD

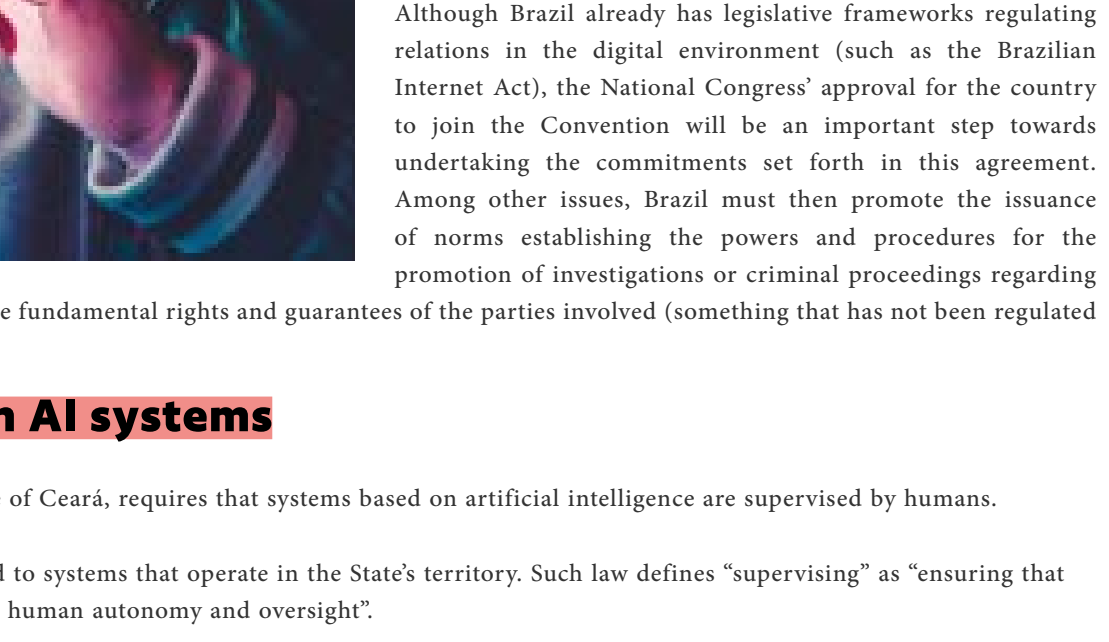
In this edition, we produced a special content in celebration of the first year of LGPD (Brazilian General Data Protection Law). Throughout this year, we have witnessed the beginning of a journey, a new perspective on privacy and data protection...



Data Protection Litigation over the First Year of LGPD. Main topics: Data leakage, improper sharing, abusive treatment, etc. Judiciary: More than 1,090 decisions, 80% increase in court decisions in just 2 months.

PEC addressing data protection is approved by House of Representatives

On August 31, 2021, the House of Representatives approved the Bill of Constitutional Amendment (PEC) No. 17/2019 by 439 votes in favor and 1 against.

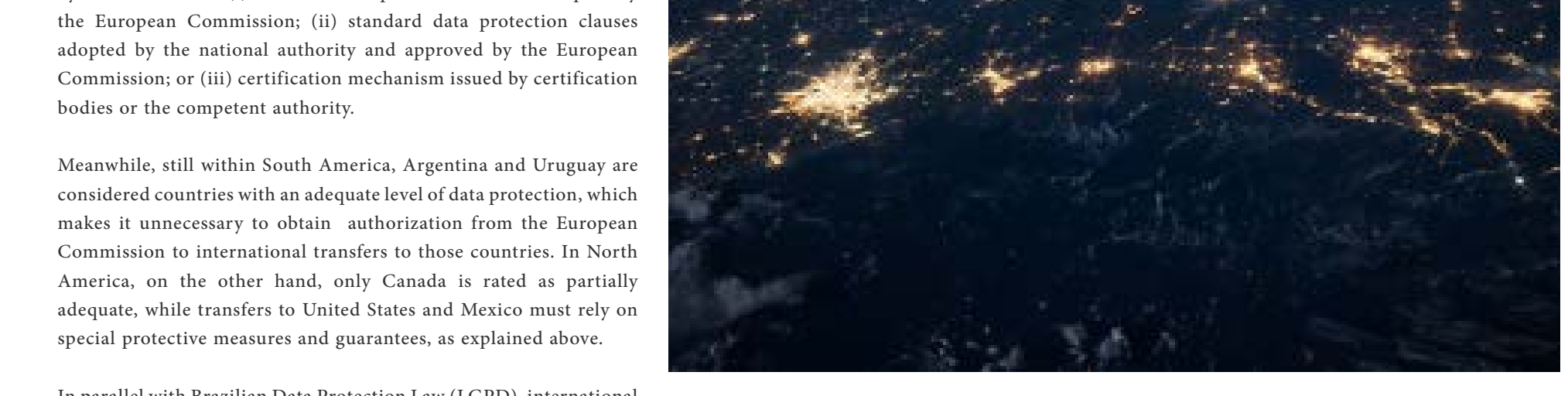


ANPD's regulation on the application of the LGPD for micro and small enterprises is presented for public consultation and discussion at a public hearing

In line with the schedule set forth with its Regulatory Agenda, the National Data Protection Authority (ANPD) published on August 30 its first draft resolution regulating the application of the Brazilian General Data Protection Law (LGPD).

In its preliminary resolution (available at the following link), the ANPD sets forth specific mechanisms to ease the process of adaptation to the LGPD for these small-sized data processing agents.

Considering this scenario, civil society is invited to participate in the ANPD's public consultation through the 'Participa + Brasil' platform (available at the following link).



The process of Brazil's accession to the Budapest Convention on Cybercrime has begun

On August 18, the House of Representative's Committee of Constitution and Justice (CCJ) approved a favorable report on Brazil's accession to the Budapest Convention, which was then submitted to the House of Representatives for analysis and voting.

The Budapest Convention was originally signed in 2001 by the Council of Europe and, in direct connection to the changes triggered by the growing digitalization, it is presented in the international scenario as an important instrument to deal with the fight against cybercrime.

Although Brazil already has legislative frameworks regulating relations in the digital environment, such as the Brazilian Internet Act, the National Congress' approval for the country to join the Convention will be an important step towards undertaking the commitments set forth in this agreement.

Among other issues, Brazil must then promote the issuance of norms establishing the powers and procedures for the formal in cloud-based environments, such as security incidents, data hijacking and unauthorized access to personal data.

Requirement for human supervision in AI systems

The Law No. 17,611/2021, approved by the Legislative Assembly of the State of Ceará, requires that systems based on artificial intelligence are supervised by humans.

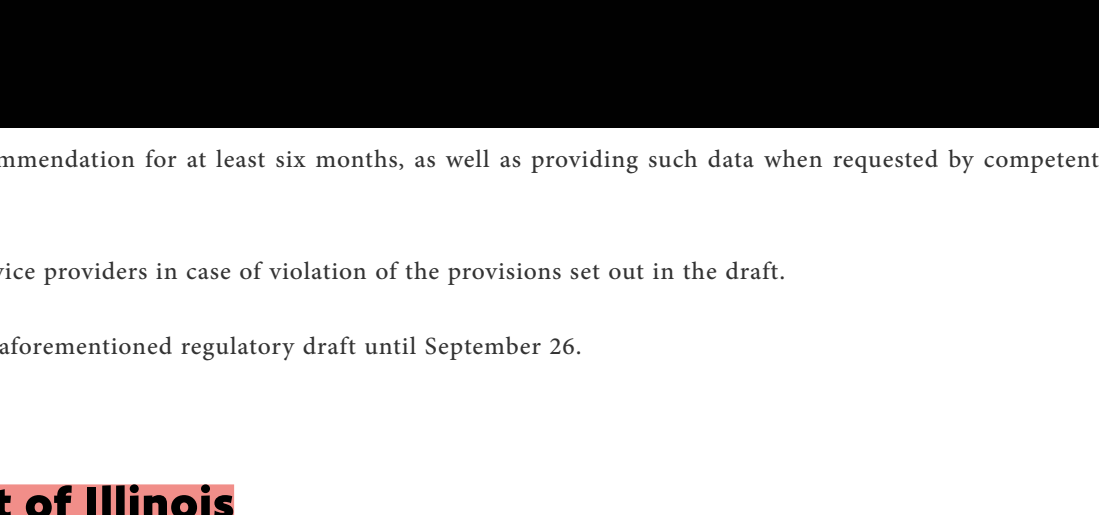
Law No. 17,611/2021 is applicable to companies headquartered in Ceará and to systems that operate in the State's territory. Such law defines "supervising" as "ensuring that systems are always managed by and subject to humans, in order to maintain human autonomy and oversight".

It is worth noting that human review of automated processes, which are essentially performed by artificial intelligence, was provided in the original wording of the Brazilian General Data Protection Law (LGPD); however, this provision was vetoed by the President of the Republic.

The Law follows the worldwide trend of trying to regulate biases often reproduced by artificial intelligence. Such programs may often reproduce biases and prejudices of the people who programmed them, or the database used to train the algorithm.

French Authority's world data protection map

The world_data_protection_map of the French Data Protection Authority (Commission Nationale de l'Informatique et des Libertés or CNIL) classifies countries according to their level of adequacy - adequate, partially adequate and not adequate country - with regard to data protection rules of General Data Protection Regulation (GDPR), as well as presents the applicable national law and the national competent authority of each country.



With respect to Brazil, CNIL understands that the country does not have an adequate level of data protection. In other words, the Brazilian data protection ecosystem does not meet GDPR's standards.

In parallel with Brazilian Data Protection Law (LGPD), international treaties that provide an adequate degree of protection of personal data compatible with LGPD's rules - such as countries or international bodies that provide an adequate degree of protection of personal data compatible with LGPD's rules - are listed and classified by the Brazilian Data Protection Authority (ANPD).

Guidance on the requirements cookies consent

The Maltese National Data Protection Authority (Information and Data Protection Commissioner) published, at the end of August, guidance on obtaining consent for the use of cookies on data subjects' electronic devices.

Initially, the Maltese Authority established that the applicable legal basis for the use of cookies is the prior and informed consent of the data subject. Hence, it is required a valid consent mechanism whereby an affirmative action is provided by the data subject, indicating its authorization.

In light of General Data Protection Regulation (GDPR), processing agents must ensure that: the consent has been freely given, in a specific and informed way, as result of unambiguous indication of data subject's interests and the consent can be revoked.

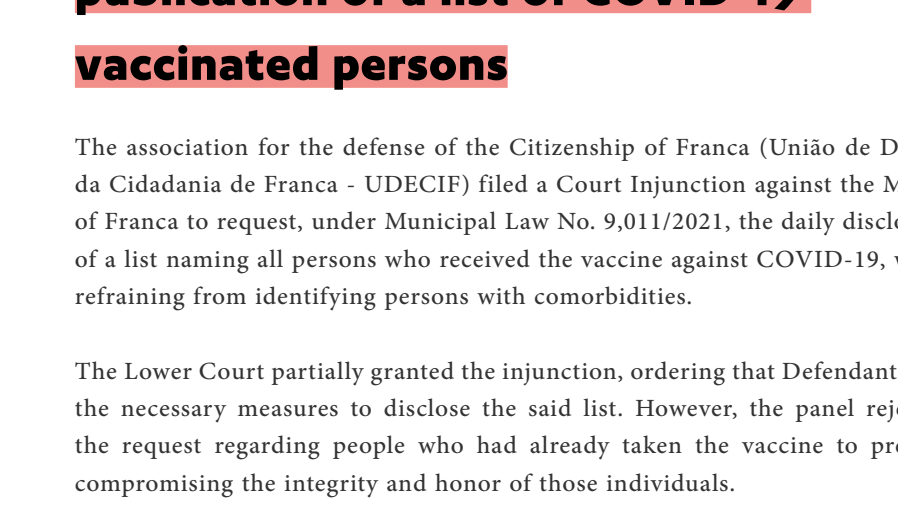
The Maltese Authority is guided by the principle of transparency, which aims for the provision of basic information about the processing of personal data to its respective holders, including information about exercising rights, especially revocation of consent.

In addition, a list of practices that are not considered adequate to the data protection rules was also made available: (i) "cookie wall", a banner that only allows users and visitors to websites and applications to access them after they provide consent for all cookies; (ii) "opt-in" and pre-selected or pre-filled fields with answers that automatically indicate the data subject's consent; (iii) "scrolling" tacit obtaining of consent based on swiping through webpages.

As highlighted above and in accordance with Brazilian Data Protection Law (LGPD), consent is a free, informed and unambiguous manifestation in which the data subject agrees to her/his processing of personal data for a given purpose. This consent must be in writing or by other means that demonstrate the expression of will of data subject.

Brazilian Data Protection Authority (ANPD) is expected to provide specific guidelines on obtaining consent; meanwhile, the guidelines set out above are fully applicable to the Brazilian reality.

Guidelines for cloud-based environments' security



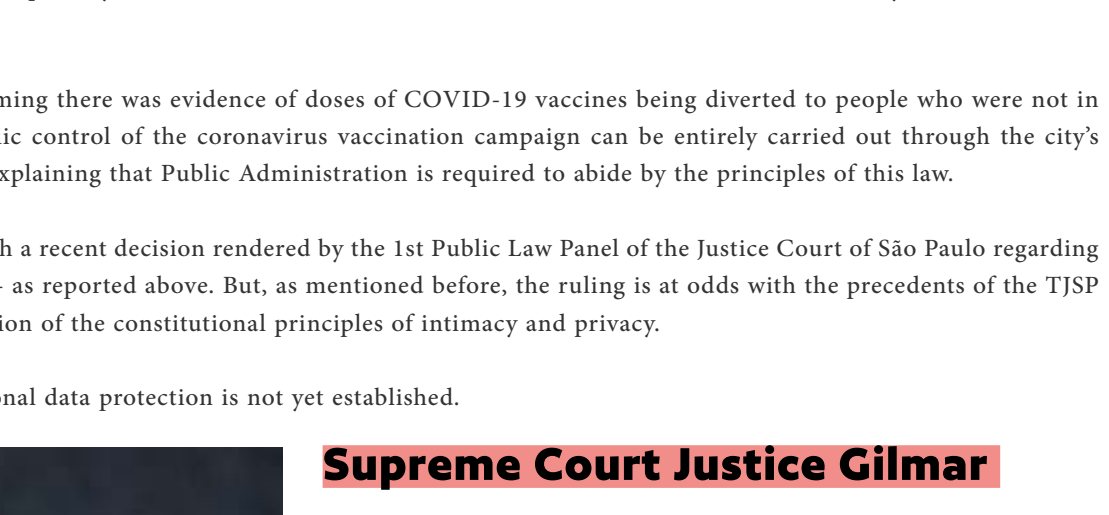
In guidelines on security measures for cloud-based environments, such as cloud-based storage systems, the Irish Data Protection Authority has drawn up five (5) steps to mitigate common risks found in cloud-based environments, such as security incidents, data hijacking and unauthorized access to personal data.

on appropriate technical security measures for the protection of personal data. In any case, the recommendations made are perfectly applicable and compatible with the Brazilian data protection rules.

In general, the Irish Authority recommends that processing agents implement a specific policy for security environments and apply multi-layered technical and organizational measures, such as access control, firewall, antivirus, employee training, policy planning and development.

Cyberpace Administration of China publishes a draft regulation on algorithmic recommendations and solicits public opinion

On August 27, 2021, the Cyberpace Administration of China (CAC) published the new normative draft to regulate the recommendations of algorithms for internet information services platforms.



The draft has several duties and responsibilities applicable to algorithm recommendation service providers. For instance: a) observing morals and social ethics, respect commercial ethics and professional ethics, as well as respect the principles of equality and transparency; b) prohibiting the use of algorithm recommendation services to engage in activities that undermine national security, public order, the legal interest of individuals and to disclose sensitive information; c) strengthening content recommendation in order to identify illegal and harmful information; d) clearly notifying users of the status of algorithm recommendation services.

The first step for mitigation would be (i) access control and the use of two-factor authentication, with the requirement of high difficulty passwords. The second step involves (ii) reviewing security settings selected by default to ensure that security measures are being properly applied and in accordance with the needs of each agent.

Regarding the provision of the algorithm recommendation service for minors, the draft provides for the obligation to comply with the duties of online protection of minors in accordance with applicable Chinese laws, in addition to making it convenient for minors to obtain informative content beneficial for their age.

Meanwhile, the third stage concerns (iii) the assistance and open and constant dialog with information technology services, whether internal or external, in order to verify that the security measures adopted are up to date and effective.

The draft also provides that algorithm recommendation service providers must improve the recommendation mechanisms and preserve information, in particular the daily history of the algorithm recommendation for at least six months, as well as providing such data when requested by competent bodies.

The fourth step (iv) aims to ensure that the employees of the processing agents have been properly trained about security incidents and physical and digital threats. Such training should be periodically conducted and updated. Additionally, agents should provide clear policies on the use of cloud-based environments.

Finally, the draft also establishes a fine of 5,000 to 30,000 yuan to these service providers in case of violation of the provisions set out in the draft.

Finally, the last step (v) recommends that agents monitor the categories of data stored in cloud-based environments, as well as classify such data to ensure that appropriate and adequate measures were applied.

In this sense, CAC will be open to receive public opinion in relation to the aforementioned regulatory draft until September 26.

As pointed out in the previous item, the Brazilian Data Protection Authority (ANPD) is expected to provide technical guidelines on obtaining consent; meanwhile, the guidelines set out above are fully applicable to the Brazilian reality.

The Protecting Household Privacy Act of Illinois

The General Assembly of the State of Illinois recently enacted the Public Act No. 102-0597, named the Protecting Household Privacy Act. The document regulates the access and use of a private household's electronic data by law enforcement.

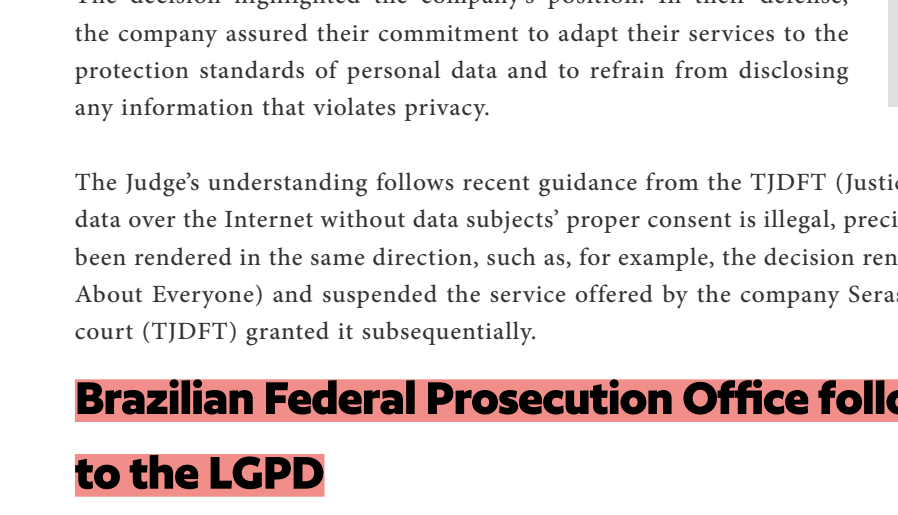
In greater detail, the Act, which will be effective January 1, 2022, states that a law enforcement agency cannot obtain electronic communication from devices within a household without a court order based on probable cause or unless voluntarily provided by the house owner. Other exceptions are listed on the Section 15 of the Act.

The Act also dictates case data retention. If a law enforcement agency obtains household electronic data, it may be retained if it is suspected evidence of criminal activity or relevant to an ongoing case, otherwise it shall be destroyed within 30 days.

The same principle applies to data disclosure. If a law enforcement agency obtains household electronic data, the agency shall only disclose the information obtained to a third party if the information is relevant to a criminal proceeding or investigation by a grand jury, or with the lawful consent of the owner of the household electronic device.

Lastly, the Act establishes that if a court finds that a law enforcement agency used household electronic data as evidence, and that such data was obtained in violation of the Act, then the information shall be presumed to be inadmissible in any judicial or administrative proceeding.

Brazilian Superior Electoral Court amends art on disclosure of member data



In compliance with the General Data Protection Law (LGPD), TSE (Brazilian Superior Electoral Court) amended article 26 of TSE Resolution No. 23,596/2019, which provides for the publication of a listing of personal data of political party affiliates for general open consultation.

The current understanding of the Justices is as follows: (i) absence of unequivocal proof of damage to consumers under a description of circumstances, which would not go beyond mere annoyance, and (ii) absence of proof of interference or fault of the construction company in the alleged improper transfer or leakage of personal data, which removes the causal link to justify the original sentence.

According to Court Chief Justice Luis Roberto Barroso, the Resolution will (i) restrict the disclosure of data to the period during which candidates are selected and contested; (ii) cover only the disclosure of information on affiliate names and (iii) provide a report to cover the party-switching of deputies, councilors and their alternates, allowing those with legitimate causes to file suit for loss of mandate.

Justice Court of São Paulo State overturns judgment against construction company for alleged personal data leaks

The 3rd Private Law Panel of the Justice Court of São Paulo State amended a ruling issued by the lower court to exempt a construction company from paying compensation to its consumers, ruling out the enforcement of the LGPD. By applying the general rule of non-retroactivity of the law, the alleged violation of provisions in the LGPD was rejected, and the absence of unequivocal proof that the company had improperly passed on personal consumer data to third parties was taken into consideration.

These changes in party affiliation have been carried out to protect affiliates and mitigate possible damages to holders of personal data, while preserving the right of party affiliation; the affiliate list will no longer be available for public consultation.

The original judgment ordered the construction company to pay damages totaling BRL 10,000.00 for alleged third-party consumer personal data with other companies - financial institutions and internet decoration businesses.

The current understanding of the Justices is as follows: (i) absence of unequivocal proof of damage to consumers under a description of circumstances, which would not go beyond mere annoyance, and (ii) absence of proof of interference or fault of the construction company in the alleged improper transfer or leakage of personal data, which removes the causal link to justify the original sentence.

These changes in party affiliation have been carried out to protect affiliates and mitigate possible damages to holders of personal data, while preserving the right of party affiliation; the affiliate list will no longer be available for public consultation.

The decision, which is still subject to appeal, demonstrates a significant result of the recent position of the TJSP in an attempt to curb sentences for unreasonable damages based on alleged violations of the LGPD, seeking proper enforcement based on reasonableness and considering the concrete case.

Justice Court of São Paulo State revokes injunction ordering the publication of a list of COVID-19 vaccinated persons

The association for the defense of the Citizenship of Franca (União de Defesa da Cidadania de Franca - UDEFICF) filed a Court Injunction against the Mayor of Franca to request, under Municipal Law No. 9,011/2021, the daily disclosure of a list naming all persons who received the vaccine against COVID-19, with the lowering of identifying persons with comorbidities.



The lower court partially granted the injunction, ordering that Defendant took the necessary measures to disclose the said list. However, the panel rejected the request regarding people who had already taken the vaccine to prevent compromising their integrity and honor of those individuals.

The Petitioner then filed an Interlocutory Appeal arguing that the disclosure of said list would not violate the integrity and honor of the persons listed, since the Access to Information Law and the LGPD granted the Public Administration the right to disclose personal data, subject to the public interest and the enforcement of governmental policies.

These changes in party affiliation have been carried out to protect affiliates and mitigate possible damages to holders of personal data, while preserving the right of party affiliation; the affiliate list will no longer be available for public consultation.

In turn, the 1st Public Law Panel of the Justice Court of São Paulo State (TJSP) denied the appeal, essentially prohibiting the publication of data on any vaccinated people. According to the Court, Municipal Law No. 9,011/2021 is contrary to the provisions under article 5-X of the Federal Constitution and the LGPD provisions regarding the data privacy and processing solely under one of the legal bases described in art. 7 of the LGPD.

In addition, the panel mentioned that the purpose of the municipal rule (to curb possible illegalities) could be achieved by other means, such as sending the lists to the Public Prosecution Office, the body responsible for defending the legal order, the democratic regime, and the unsalvageable social and individual rights.

Concerning banking data - connection records, access records and the content of private communications -, the Justice explained that said data is protected by the fundamental right to privacy and protection of personal data. The Justice also mentioned the paradigmatic ADI 6389, relating that this constitutional protection involves, from a subjective perspective, the protection of individuals against the risks threatening their personality as a result of the collection, processing, use, and circulation of personal data; and, from an objective perspective, this allows individuals to control the flow of their data (informational self-determination).

Specifically regarding fiscal and banking data, the Justice understood that the lifting of secrecy must be upheld provided that it is limited in time and that the information collected remains under the custody of the CPI President, Omar Aziz, who may provide access by the Colleague to documents related to the Commission's investigation only during a meeting in chambers.

Supreme Court Justice Gilmar Mendes restricts lifting bank and tax secrecy based on Data Protection

Justice Gilmar Mendes, of the Federal Supreme Court (STF), partially granted a preliminary injunction in a Writ of Mandamus (MS 38,187) filed by a video production company against the Parliamentary Inquiry Commission (CPI) on the Pandemic, to (i) suspend the lifting of confidentiality on telematic and telephone data - until the final decision in the Plenary of the STF; and (ii) uphold the lifting of the company's banking data - connection records, access records and the content of private communications -, the Justice explained that said data is protected by the fundamental right to privacy and protection of personal data. The Justice also mentioned the paradigmatic ADI 6389, relating that this constitutional protection involves, from a subjective perspective, the protection of individuals against the risks threatening their personality as a result of the collection, processing, use, and circulation of personal data; and, from an objective perspective, this allows individuals to control the flow of their data (informational self-determination).

Concerning banking data - connection records, access records and the content of private communications -, the Justice explained that said data is protected by the fundamental right to privacy and protection of personal data. The Justice also mentioned the paradigmatic ADI 6389, relating that this constitutional protection involves, from a subjective perspective, the protection of individuals against the risks threatening their personality as a result of the collection, processing, use, and circulation of personal data; and, from an objective perspective, this allows individuals to control the flow of their data (informational self-determination).

PROCON/MS fines the business for violating the LGPD in contracting payroll-deductible loans

The Consumer Protection Agency in the State of Mato Grosso do Sul (PROCON/MS) fined a consulting and insurance brokerage firm after finding in a due diligence procedure, likely violations of the LGPD in payroll-deductible loan contracts.

The business posted advertisements describing how easy it was to obtain cash through payroll-deductible loans based on FGTS (Brazilian Government Savings Incentive Fund), without consulting credit protection agencies, provided that applicants/consumers disclosed their personal data.

PROCON found that this requirement was accompanied either by any documentation proving consumers' willingness or consent to their data processing nor by any restriction to using this data for a specific purpose.

PROCON/MS fined a consulting and insurance brokerage firm after finding in a due diligence procedure, likely violations of the LGPD in payroll-deductible loan contracts.

Because of the irregularities, PROCON/MS set a deadline for the submission of justifications and the presentation of a legal defense, and only afterward PROCON/MS will decide on the application of any penalties.

PROCON-SP demands clarifications from banks and fintechs about the invoice scam

Cases related to the so-called "invoice scam" have increased recently. In the said scam, criminals use data such as (i) names, social security numbers, and (ii) phone numbers to send messages or potential victims, offering to negotiate an alleged debt, or even giving discounts on cash payments on a card invoice. Upon clicking on a link in the message, victims are redirected to pages that mimic the websites of banks and fintechs and issue fake bills.

Cases related to the so-called "invoice scam" have increased recently. In the said scam, criminals use data such as (i) names, social security numbers, and (ii) phone numbers to send messages or potential victims, offering to negotiate an alleged debt, or even giving discounts on cash payments on a card invoice. Upon clicking on a link in the message, victims are redirected to pages that mimic the websites of banks and fintechs and issue fake bills.

Given this increased number of cases, PROCON-SP (Consumer Protection Agency in São Paulo) notified banks and financial institutions and gave them 72 hours, as of September 8, to register, report and describe the security mechanisms they adopt to allow consumers to verify the authenticity of fake bills sent to them.

Additionally, the consumer protection and defense agency questioned whether other measures and action plans have been developed to prevent new cases from occurring. Finally, the notification required banks to clarify the measures taken upon the occurrence of fraud, both individually and collectively.

Justice Court of the Federal District and State Territories suspends website that sells personal data

The Public Civil Action filed by MPDEF (Brazilian Federal District and Territories Public Prosecution Office) was granted in court to order the company responsible for the facultativirtual.com.br domain to refrain from selling personal data and eliminate all personal data retention of the Brazilian Personal Data Base.

The MPDEF stated the company sold personal information provided to several users - such as name, address, phone number, e-mail address and even their profession - to companies interested in promoting targeted Internet advertising. Given this and based on the legal provisions established in the LGPD, in the CDC (Consumer Defense Code), and in the Federal Constitution, the Judge a quo ruled on the company's unlawful practice, since consumers did not provide their express consent to process their personal data.

The decision highlighted the company's position. In their defense, the company assured their commitment to adapt their services to the protection standards of personal data and to refrain from disclosing any information that violates privacy.

The Judge's understanding follows recent guidance from the TIDFET (Justice Court of the Federal District and State Territories), which has considered that the sale of personal data over the Internet without data subjects' proper consent is illegal, precisely due to the apparent violation of privacy and intimacy. In this sense, previous rulings have already been rendered in the same direction, such as, for example, the decision rendered by the 3rd Civil Court of Brasília that blocked a website called "Tudo sobre Todos" (Everything About Everyone) and suspended the service offered by the company Serasa Experian - the service suspension was initially denied by the lower court. However, the appellate court (TIDFET) granted it subsequently.

Brazilian Federal Prosecution Office follows other institutions in the public sphere and adapts to the LGPD

The "services" page of the MPF (Brazilian Federal Prosecution Office) website now includes a form through which personal data subjects can request information on the existence and any processing of their data carried out by the MPF. According to the LGPD, citizens are entitled to verify, free of charge, which of their data was collected, how said data is stored, and even request the deletion of their data.

The "services" page of the MPF (Brazilian Federal Prosecution Office) website now includes a form through which personal data subjects can request information on the existence and any processing of their data carried out by the MPF. According to the LGPD, citizens are entitled to verify, free of charge, which of their data was collected, how said data is stored, and even request the deletion of their data.

This initiative came after the TJSC (Justice Court of Santa Catarina State) launched LGPD last month, an application to make it easier for citizens to file requests related to privacy and protection of their data within the scope of the Courts of Santa Catarina State.

Newsletter content produced by TozziniFreire's Cybersecurity & Data Privacy practice.

PARTNERS RESPONSIBLE FOR THE CONTENT:
- Marcela Waksman Ejnisman
- Patricia Helena Marta Martins
- Carla do Couto Hellu Battilana
- Bruna Borghi Tomé

For further information, please visit: tozzinifreire.com.br/

This material may not be reproduced, in whole or in part, without prior consent and permission of TozziniFreire Advogados.