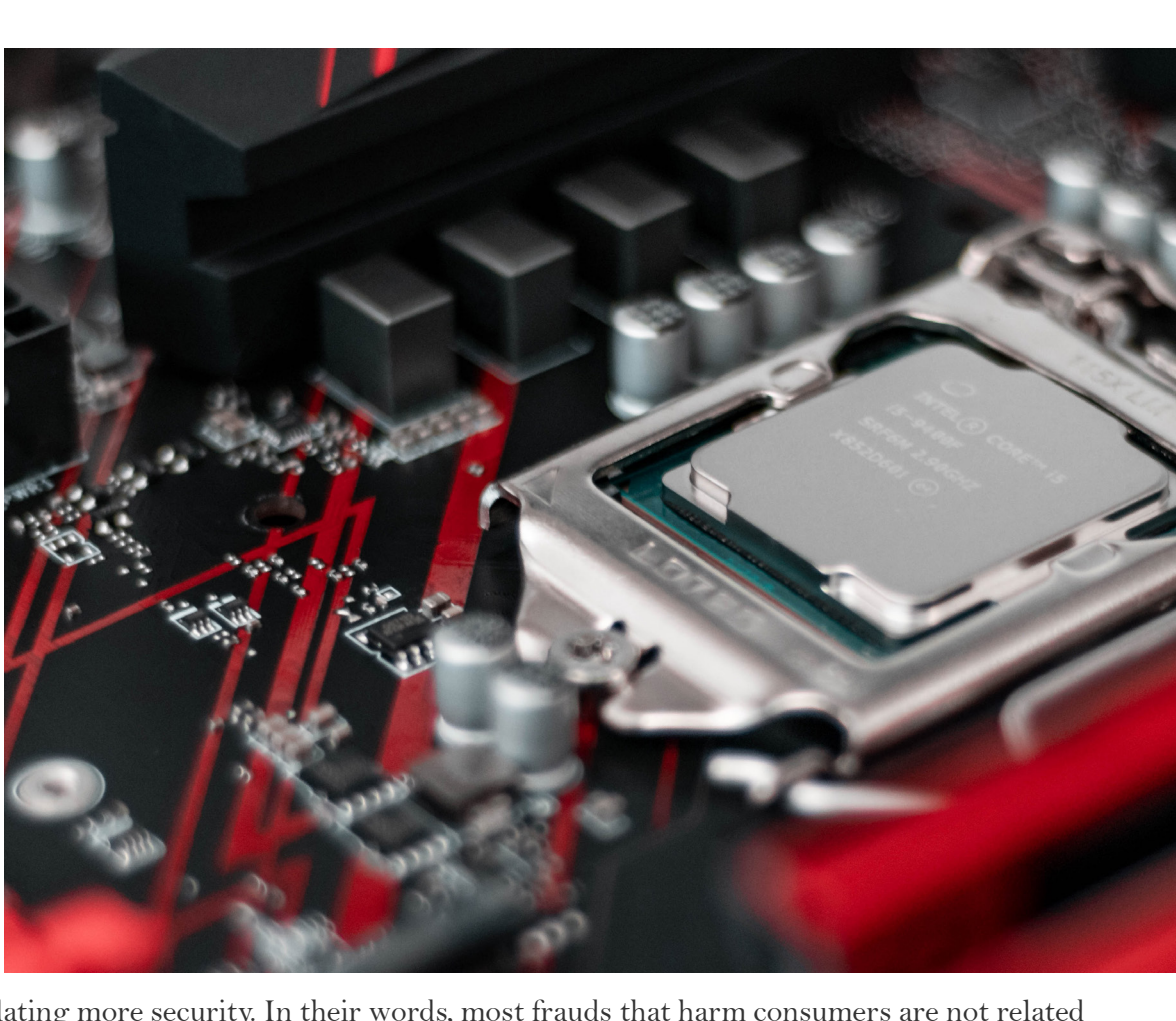
TF cybernews
9th edition | 2021
TOZZINIFREIRE ADVOGADOS

Brazilian Context

Electronic means of payment industry supports Bill that discusses storage of consumer data by providers



Representatives of the electronic means of payment industry have supported the new version of Bill No. 786/2019, which discusses the storage of consumer payment data by service providers and product suppliers, pending before Consumer Defense Commission of Brazilian Chamber of Deputies. It is important to note that the previous version of the Bill prohibited the storage of data relating to credit and debit cards and other means of payment, without the consumer's prior authorization.

Under the original terms of the Bill, if the data subject consented to the storage, this authorization would be valid for a period of twelve (12) months, with the possibility of revocation at any time. It is also noteworthy that, with the consumer's consent, the service provider and product supplier could not use the data for new purchase operations, nor transfer them to third parties, without the data subject's prior authorization.

During the Commission's debate, the representatives argued that Brazilian General Data Protection Law (LGPD) already sufficiently provides for consumer security and that there is already strong regulation about these transactions by Brazilian Central Bank. As the representatives pointed out, the original text of the Bill would lead to too much bureaucracy, without stimulating more security. In their words, most frauds that harm consumers are not related to data storage by payment institutions.

In this regard, the industry representatives also highlighted the market growth, during the first three months of 2021, with a 17.3% increase in transactions with credit, debit, and prepaid cards, totaling more than BRL 500 billion, compared to the same period last year. Finally, it was highlighted the 35.6% increase in remote purchases, in the first quarter of this year, reaching more than BRL 120 billion, which could be negatively impacted by the original Bill, according to the industry representatives.

Brazilian National Data Protection Authority creates its Governance Committee

At the beginning of July, Ordinance No. 15/2021 of Brazilian National Data Protection Authority (ANPD) was published in Brazilian Official Gazette, establishing its Governance, Risks and Controls Committee (Governance Committee).

Under the terms of Article 1, Committee will be composed of the Chief Executive Officer and the Directors of ANPD, who may appoint their substitutes to act in cases of absence or impediment. As determined by the provision, Executive Secretary of the Committee will be General Secretariat of ANPD.

The Ordinance also states that it will be the Committee's responsibility to define institutional strategies and strategic guidelines on public governance, risk management, transparency and integrity, planning, internal control mechanisms, and efficient administrative management.

Article 3 of the Ordinance establishes as competences of Governance Committee the orientation of the high administration in the implementation and maintenance of processes, structures and mechanisms adequate to the incorporation of the principles and guidelines of governance; the incentive and promotion of initiatives that seek to implement the monitoring of results in the body, that promote solutions for the improvement of the institutional performance or that adopt instruments for the improvement of the decision-making process; the promotion and monitoring of the implementation of measures, mechanisms and organizational practices of governance defined by Interministerial Governance Committee; and the elaboration of technical manifestation related to the themes of its competence.

Ultimately, the final articles of Ordinance state that the Committee will meet monthly and that a quorum of two-thirds of the representatives is required, which will take place with a simple majority and the President's casting vote.

Urgency regime for Brazilian artificial intelligence Bill has been approved

The Brazilian Chamber of Deputies has approved earlier this month the urgency regime for Bill 21/2020, which provides principles, rights and duties for the use of artificial intelligence in Brazil. In accordance with the Bill, the artificial intelligence system would be the system based on a computational process capable of, for a given set of objectives defined by humans, making predictions and recommendations or taking decisions that influence real or virtual environments.

Different figures related to the use of artificial intelligence are also discussed, such as artificial intelligence agents, which include development agents, responsible for planning and implementing the artificial intelligence system, and operation agents, responsible for monitoring and operating the system.

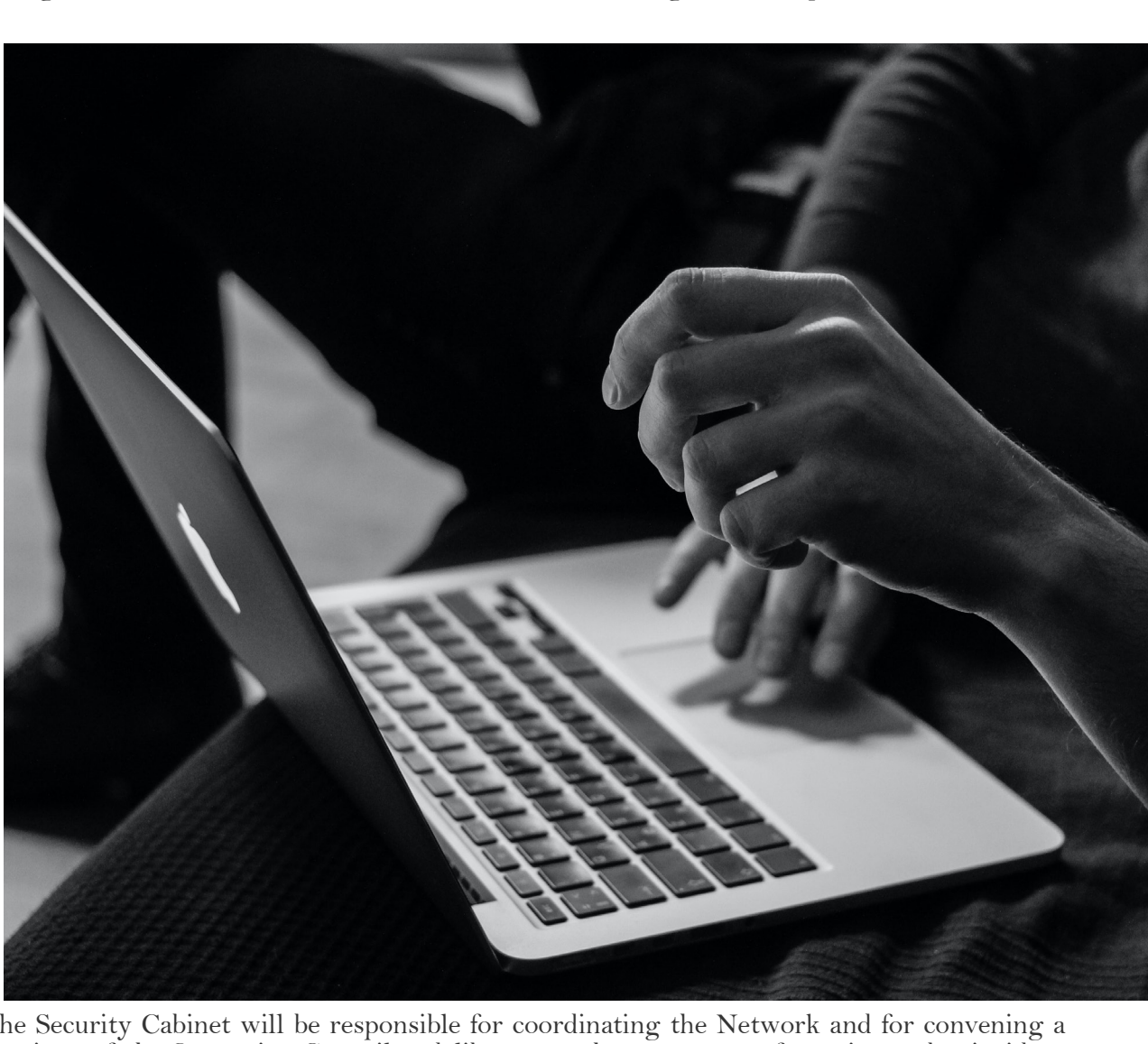
Among the fundamentals of the use of artificial intelligence, the Bill foresees: technological development and innovation; free initiative and free competition; respect for human rights and democratic values; equality, non-discrimination, plurality and respect for labor rights; and privacy and data protection. Its principles encompass purpose limitation, human-centeredness, non-discrimination, transparency and explainability, security, and accountability and responsibility.

The Bill also establishes the rights of interested parties – all those involved in or affected, directly or indirectly, by artificial intelligence systems –, specifically the right to science from the institution responsible for the artificial intelligence system; access to clear and adequate information about the criteria and procedures used by the artificial intelligence system that adversely affect them; and access to clear and complete information about the use, by the systems, of their sensitive data, without prejudice to the rights granted to the data subjects by the General Law of Data Protection (LGPD).

It is worth mentioning that the use of artificial intelligence is directly related to automated decisions, which, according to the LGPD, guarantee the right of the data subject to review the decisions that affects their rights and interests (art. 20, LGPD).

Cyber Incident Management Federal Network has been established

Decree No. 10,748/2021 was published in the Brazilian Federal Official Gazette on July 19. It regulates the establishment and operation of the Cyber Incident Management Federal Network (Network), based on the provisions of the National Information Security Policy (Decree No. 9,637 of December 26, 2018), with the main function of coordinating bodies and legal entities of the Federal Government, autonomous agencies and public foundations, for the prevention, processing and response to cyber incidents.



The objectives of the Network encompass: dissemination of measures for prevention, processing, and response to cyber incidents; sharing of alerts on cyber threats and vulnerabilities; dissemination of information on cyberattacks; promotion of cooperation among Network's participants; and promotion of speed in the response to cyber incidents.

Decree No. 10,748/2021 establishes several definitions related to the composition of the Network, of which we highlight: team of prevention, processing and response to cyber incidents, person in charge of providing services related to cybersecurity for the Federal Government; sectorial coordination team, person responsible for the prevention, processing and response to incidents of the regulatory agencies, Central Bank of Brazil, National Nuclear Energy Commission or its regulated entities in charge of coordinating activities of cybersecurity and centralizing the notifications of incidents of the other teams of the regulated sector; and cyber incident, an occurrence that compromises, definitely or potentially, the availability, integrity, confidentiality or authenticity of an information system or of information processed, stored or transmitted by such system, which can also be characterized by the attempt to exploit the vulnerability of an information system that constitutes a violation of law, security policy, security procedure or policy of use.

Concerning its composition, the Network will be composed by the Institutional Security Cabinet of the Presidency of the Republic, by the bodies and legal entities of the Federal Government – mandatory participation – and by the public companies and government controlled company and their subsidiaries – optional participation. The Security Cabinet will be responsible for coordinating the Network and for convening a meeting of the Foreign Relations and National Defense Committee of the Governing Council to deliberate on the occurrence of a serious cyber incident or when a high cyber risk is identified.

Finally, Decree No. 10,748/2021, effective as of the date of its publication, provides a series of obligations that must be met by the Brazilian Federal Government, as well as specific obligations to regulatory agencies, the Central Bank of Brazil and the National Nuclear Energy Commission.

Guidelines

Guidelines on the application of administrative fines

With the effective date of the administrative sanctions provisions of the Brazilian Data Protection Law (LGPD) in August this year, we recall some of the principles and criteria brought forward by the European Data Protection Board (EDPB) in its guideline on the application and framing of administrative fines for the purposes of the General Data Protection Regulation (GDPR). Administrative fines, for the EDPB, are considered central elements for the implementation of the new data protection regime introduced by the GDPR.

According to EDPB, the imposition of fines must be guided by a series of principles, of which we stand out: equivalent sanctions, which aim for the uniformity and consistency in the levels of data protection in European countries, characteristics that can be achieved by cooperation between these countries, even if the authorities are independent from each other; effective, proportional and dissuasive sanctions, which must objectively correspond to the nature, gravity and consequences of the breach; and evaluation of the specific case and its peculiarities.

The EDPB also clarifies some criteria for the application of the fine, which encompasses: the nature, gravity and duration of the breach; the occurrence of intentional or merely negligent unlawful conduct; the actions taken by the processing agents to mitigate the damage caused; the degree of responsibility of the processing agents to adopt technical and organizational data protection measures; the existence of previous breaches; the degree of cooperation with the data protection authority in order to remedy the breach's consequences; the categories of personal data affected; the manner in which the authority learned about the breach, for example, whether there was notification of the breach from the controller; compliance with measures previously directed to processing agents on the same matter; and other aggravating or mitigating factors, such as financial advantages gained or losses avoided in relation to the breach.

The principles and criteria aforementioned may also be taken into account in the application of future sanctions, including fines, by the Brazilian National Data Protection Authority (ANPD) arising from any violations of the provisions and obligations established by the LGPD. Specifically, regarding the criteria addressed, LGPD in its article 52 already establishes parameters and criteria for the application of sanctions, which, in addition to the criteria pointed out by EDPB, consider the good faith of the offender, its economic condition and the adoption of good practices and governance policies.

Proposal for a regulation on markets in crypto-assets in light of data protection

The European Data Protection Supervisor (EDPS) issued, at the end of June, its opinion on the Proposal for a Regulation on Markets in Crypto-assets. The Proposal, in sum, sets out transparency requirements for the issuance and admission of crypto-assets trading, rules on authorization and supervision of crypto-assets service providers, consumer protection rules related to the issuance, trading, exchange and custody of crypto-assets, among other provisions.

In light of the provisions of the General Data Protection Regulation (GDPR), EDPS highlighted the need of reflection about the impact of data protection rules and principles on underlying technologies of crypto-assets, such as blockchain and distributed ledgers (DLT). EDPS also pointed out the responsibility of the European Parliament to ensure that the processing activities arising from the Proposal is carried out in compliance with data protection, as well as the liability of data controllers to ensure the compliance with GDPR's accountability principle.

Considering that the data controllers in the context of crypto-assets would be their issuers – any legal entity offering any type of crypto-assets to the public or seeking admission of them into trading platforms –, EDPS recommends the explicit designation the issuers as data controllers in the Proposal's text. As a result, issuers would have a legal obligation to conduct a Data Protection Impact Assessment, in addition to other obligations related to safeguards for data subjects, in the case of crypto-assets' purchasers or (investors).

Moreover, EDPS emphasizes the need of providing privacy notices to data subjects and addresses the most appropriate legal bases for processing personal data raised from the issuance of and transactions of crypto-assets – the performance of a contract or of preliminary proceedings related to a contract to which the data subject is party and the compliance with legal or regulatory obligation by the controller.

In a parallel with the Brazilian Data Protection Law (LGPD), crypto-assets' issuers, if responsible for decisions regarding the processing of personal data, would also be framed as data controllers and would have duties related to compliance with the provisions of the LGPD, especially concerning the transparency about the processing activity performed with personal data from crypto-assets' purchasers.

Normative Developments

Japanese Amended Act on the Protection of Personal Information

Published last year, the Amended Act on the Protection of Personal Information (APPI), which updates a series of provisions regarding security incidents reporting, data sharing, international transfer and sanctions, will come fully into effect in April 2022. Part of the provisions, in particular on increasing the limits of the amount of fines – that can in some cases reach up to 100 million yen – have been into effect since December 2020.

Similar to the General Data Protection Law (LGPD), but more specific, the Amendment establishes a legal obligation to notify the Japanese data protection authority and data subjects about security incidents not only in the event of risk of damage to the rights and interests of data subjects, but also in incidents: involving sensitive personal data; capable of resulting in economic risks; occasioned by illegal purposes such as cyberattacks; or involving more than a thousand data subjects.

With regard to the international transfer of data, the Amendment incorporates new rules for its realization, of which we highlight the provision of information about the transfer to the data subjects who have consented to its realization, what includes the name of the country to which the data will be transferred, the country's data protection system and measures to be taken by the receiver of the data. It is worth mentioning that, under Japanese law, international transfer may only occur with the consent of the data subject, except in specific situations where the consent is exempted.

Furthermore, the Amendment also increases the scope of some concepts, such as personal data (or personal information), that, from now, will include pseudonymized data, i.e., data without the ability to be associated, directly or indirectly, with an individual, except by means of the use of additional information storage separately by the controller in a controlled and secure environment.

Colorado Privacy Act (CPA) has been published as the third comprehensive personal data protection legislation across USA

Colorado is the third American state to publish a comprehensive legislation regulating personal data protection at the local level (followed by California with the "California Consumer Privacy Act" - CCPA - and Virginia, with the "Virginia Consumer Data Protection Act" - VCDPA).

With the Colorado Privacy Act (CPA), the state brings forth references from other American privacy legislations, but also has its own specificities (drafted aligned with the European General Data Protection Regulation - GDPR), especially regarding the data subjects' consent.

It should be noted that the CPA applies to any legal entity that offers products and services intentionally directed at Colorado residents (provided that such companies process personal data of more than 100,000 consumers per year or have their revenue derived from the processing of data of at least 25,000 consumers).

In this regard, it is clear that this Act brings the concept of "data subject", restricting it to the consumer public and explicitly excluding from this protection individuals present in a commercial or employment relationship (such as corporate representatives and employees, among others endowed with general protection in light of data protection regulations such as the GDPR and the LGPD). In addition, although the concept of "personal data" is similar to the one adopted in Brazil (including, therefore, all information related to an identified or identifiable natural person), there is a limitation for such scope to the extent that publicly available information is excluded from the concept of "personal data".

In addition to the general rights of access, deletion, correction and portability of data, the CPA brings as a distinctive feature the power given to data subjects to actively consent. Thus, the "consent" is established as "a clear affirmative act" (i.e., not a presumed act), demonstrating the specific, free, informed, and unequivocal agreement of the data subject to the processing of their personal data. It is clear, therefore, that the rule adopted in the CPA is directly aligned with the notion of consent as an "opt-in" activity provided in both the GDPR and the LGPD (which diverges from other U.S. privacy laws that focus on the power of consent as an "opt-out" mechanism). As a result, there is an express prohibition in the CPA to obtaining consent whenever it is based on the acceptance of generic terms or with the so-called "dark patterns" (i.e., interfaces that manipulate data subjects by limiting their decision-making autonomy).

From a practical perspective, the CPA will come into force on July 1, 2023 (unlike the CCPA and the VCDPA, which will come into force on January 1, 2023), at which point the processing agents will be legally liable for the improper processing of personal data in light of this legislation. Once the Act goes into effect, the CPA will be enforceable by district attorneys and state attorneys general, which may incur in civil penalties of up to US$ 2,000 per violation (limited to US$ 500,000 whenever connected to a series of related violations).

The European Commission regulates the international personal data flow between the United Kingdom and the European Union

In light of the post-BREXIT European context, on June 28, the European Commission decided that the United Kingdom offers an equivalent standard of personal data protection to that of the European Union.

Given that the General Data Protection Regulation (GDPR) establishes specific hypothesis in which the international transfer of personal data may take place (among which there is the transfer to countries with an "adequate level of protection for personal data"), the European Commission's conclusion enables the personal data flow without the need for specific additional guarantees whenever it takes place between the European Union and the United Kingdom.

The ruling in analysis was made as a result of two decisions from the Commission regarding the UK's data protection adequacy: one based on the GDPR while the other made in light of the Law Enforcement Directive (i.e., the European regulation concerning the processing of personal data in the public security context). In this context, the Commission has concluded that the UK data protection system is still grounded on the rules that were applicable to it before BREXIT, thus incorporating the principles, rights and obligations set forth in the GDPR and in the Law Enforcement Directive.

Consequently, the aforementioned decisions also facilitate the implementation of the EU-UK Trade and Cooperation Agreement, which provides for the exchange of personal data for specific aspects, such as in judicial matter cooperation.

It should be noted, however, that the European Commission has included specific safeguards to its ruling in face of potential future disagreements. In this regard, a "sunset clause" has been put in place under the Commission's decisions, thus limiting the temporal scope regarding the understanding of the UK's adequacy level to a period of four years (being a reassessment required after this period). In addition, during these four years, the Commission will continue to monitor the UK's legislative compatibility with European data protection standards and may intervene at any time should the UK deviates from the level of protection currently in place.

Judicial Branch

Brazilian Supreme Federal Court addresses the lawfulness of court data disclosures on non-official websites

The Brazilian Federal Supreme Court (STF) acknowledged the general repercussion in Extraordinary Interlocutory Appeal (ARE) 1.307.386 (Matter 1.141), which regulates civil liabilities over the disclosure, on websites, of court information published by the official Judiciary bodies that are not subject to court secrecy.

The appeal refers to a lawsuit filed in the State of Rio Grande do Sul. The plaintiff alleged that the disclosure of information on a labor lawsuit filed by the plaintiff on a website other than the website of the Judiciary could jeopardize the plaintiff in future lawsuits. In addition, the plaintiff alleged that the information could not have been disclosed without authorization, as set forth in Resolution No. 139/2014 of the CSTJ, which determines that Regional Labor Courts limit the access to plaintiff data to prevent the creation of "black lists."

Requests for removing the plaintiff's personal and professional data from the Internet and the payment, by the defendants, of an indemnity for pain and suffering were denied by the lower and higher courts – including under the "Repetitive Resolution Incident" (IRDR) No. 70082616665. The legal basis was that "the consultation of legal information in connection with the respective lawsuits is lawful except for the name associated with lawsuits subject to secrecy, which is not applicable, as a rule, to labor lawsuits; therefore, the disclosure of information on labor lawsuits or even criminal lawsuits is not prohibited."

Despite of the favorable decision, one of the co-defendants (a legal search website) appealed before the STF requesting the decision to be enforced throughout Brazil.

In his vote acknowledging the general repercussion, Justice Luis Fux declared that the STF "shall define the extent and the meaning of the constitutional rules providing for the disclosure of court information, the right to information and for legal security, taking into consideration the right to privacy, specifically with respect to the disclosure of information on labor and criminal lawsuits, where there are search restrictions involving certain information, such as the parties' name."

The Brazilian Association of Lawtechs and Legaltechs (AB2L) requested to be included as amicus curiae. Certainly, amongst other issues, the decision could open discussions relating to possible contradictions between the right to information and informative self-determination, as set forth in the LGPD, which authorizes owners of data to control their personal data.

STF and the Marielle Franco case: general repercussion involving violation of data confidentiality has been acknowledged

The Brazilian Federal Supreme Court (STF) has acknowledged the general repercussion in Matter 1.148, which addresses the violation of confidential data from several users during the investigations of the murder of council member Marielle Franco.

The lawsuit began with a petition submitted by the Public Prosecution Office to the Rio de Janeiro State Judiciary to gain access to geographic location information from all users in the areas surrounding the crime scene, as well as from all users who performed certain Google searches before the crime.

Both the Rio de Janeiro State Judiciary (TJRJ) and the Superior Court of Justice (STJ) accepted the request to provide this data, an event that would not pose excessive risks to user privacy and intimacy.

The reporting Justice Rogerio Schietti Cruz of the STJ determined that the right to secrecy is not absolute and that this safeguard may be removed in the event of significant public interest.

The lawsuit is in progress before the STF. Upon recognition of general repercussion on this matter, this judgment may influence how criminal investigations proceed and how violation of secrecy is handled in Brazil.

Serasa found guilty for violating the LGPD

On June 24, 2021, the 5th Civil Court of Brasília, in the court records of Public Civil Lawsuit No. 0736634-81.2020.8.07.0001 filed by the MPDFT against Serasa, determined that Serasa should discontinue the sale of personal data through its "Online List" and "Client Prospecting" services.

These services comprised the creation of a customized list directed to businesses, using filters to search for new clients with characteristics in line with products and services sold by those businesses. By retaining these services, businesses obtained personal data, including names, CPF numbers (Natural Persons Register), addresses, age, gender, purchase power and socioeconomic class of individuals listed in credit protection records.

The 5th Civil Court of Brasília ordered Serasa to discontinue the sale of personal data through these services. According to the decision, despite of public disclosure of the data by owners, in which case the data owner's authorization is not required, the data owner's basic rights must be protected and, "in view of the current legal scenario," "protecting the data is required in compliance with the principles and other provisions set forth in the LGPD."

The decision is subject to appeal.

Second Civil Court of the City of Osasco, State of São Paulo: data leakage does not imply presumed moral damages

The 2nd Civil Court of the City of Osasco, State of São Paulo, in record No. 1025226-41.2020.8.26.0405, determined that possible indemnities payable to owners of data is dependent on effective proof of damages.

The Plaintiff, a member of the Personal Data Protection Institute (IPRODAPE), reported to have received information submitted by this Institute that electric power company Eletropaulo, currently named Enel, underwent a data leaking episode and, in view of this, third parties gained access to this data. The Plaintiff filed the lawsuit against the company and requested, amongst other claims, the payment for pain and suffering in the amount of R$10,000.00 (ten thousand reais). The Plaintiff alleged psychological trauma by virtue of this leak, which forced the Plaintiff to double care regarding false bill payments, in addition to being subjected to telemarketing e-mails and messages.

According to the decision, considering that the Plaintiff was unable to prove having received such e-mails, messages and calls, in addition to the fact that, getting telemarketing communications is commonplace, the request for indemnity was denied.

Furthermore, in the sentence it was determined that the claim requesting Eletropaulo, currently Enel, to provide the names of public and private entities that received such information, should be directly addressed to the National Data Protection Authority (ANPD).

The Plaintiff appealed, which decision by the Court of the State of São Paulo is currently pending.

Justice Court of São Paulo: data leakage and direct liability

The 26th Private Law Court of the State of São Paulo (TJSP) decided that company should indemnify consumer in R$ 2,000.00 (two thousand reais), based on the allegation of unlawful disclosure of personal data by the respective website. The Court applied the LGPD and reconsidered the original decision.

After shopping on the company's website, the consumer would have been advised by a third party via WhatsApp that their personal data was available on the Internet. In order to resolve the issue, the consumer asked the company to cease the disclosure of their personal data. In turn, the company took days to respond and resolve the consumer's request after the fact.

Differently from the story above, this time the TJSP determined that personal data leaks, although for a short period, would imply payment for pain and suffering. The legal basis is that personal data leaks go beyond a mere nuisance and violates the consumer's expectation that their personal data will be protected during online shopping. Accordingly, the decision determined that the company was to be held directly responsible for any possible failure in the company's electronic systems.

According to the decision, article 44 of the LGPD provides for the attribution of responsibility for possible failures of data security systems. Therefore, the Court determined that "the security failure on the company's sales website is inherent to the risk of the business itself, characterized by an unexpected event under the responsibility of the provider."

The payment of R$ 2,000.00 (two thousand reais) was calculated based on the amount paid for the on-line purchases, on the extent of the damages against the consumer and according to the parties' economic capacity. Thus far, the term for appeal by the company has not elapsed.

Although the Court determined the company's direct liability, the LGPD does not clearly establish civil liabilities applicable to the handling of data, with the understanding prevailing that liability is indirect, and depends on the evidence of damage, negligence or violation by the company when handling the data.

Fulfilling requests from owners of personal data, Justice Court of Santa Catarina launches application

Since 2018, the Santa Catarina State Judiciary (TJSC) is working to implement the General Data Protection Law (LGPD).

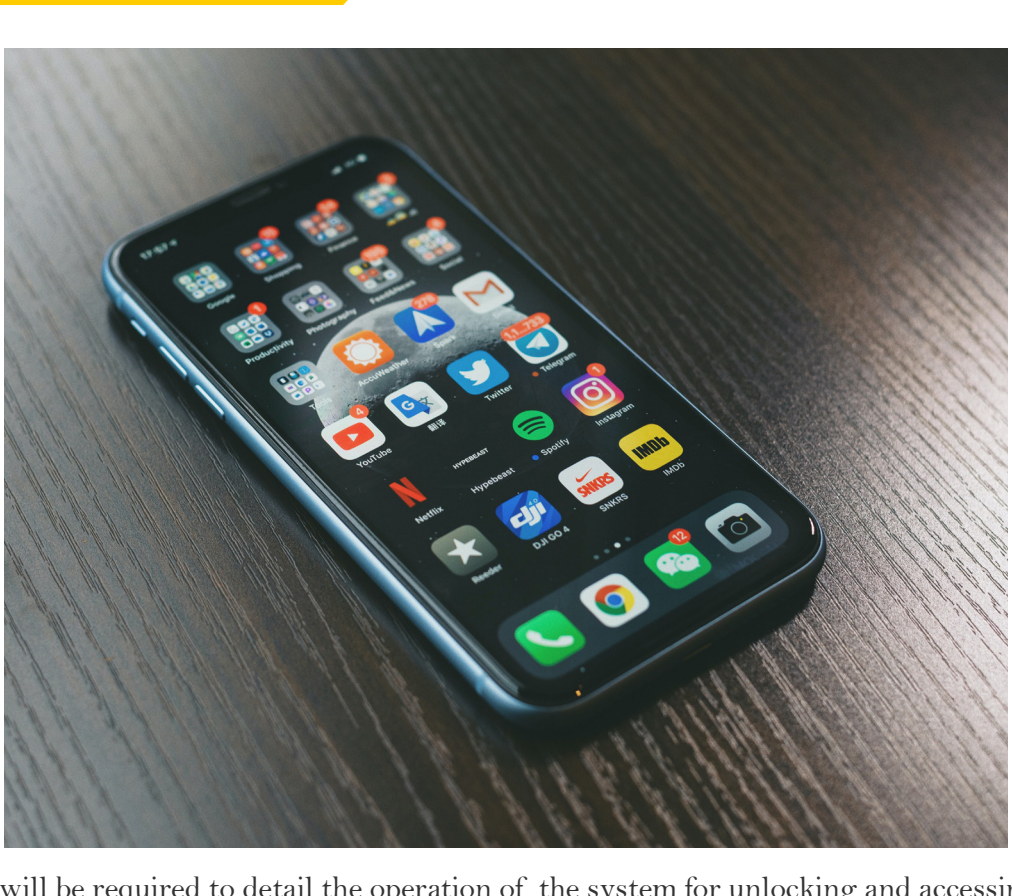
Although the authentication of the personal data owners is not mentioned in any article of the LGPD, the TJSC determined that this is an essential security requirement in response to the data owners' requests.

Accordingly, the Court determined that, in requests submitted by e-mail, telephone or electronic form, users should confirm the personal data owner's mother's name. In addition, in partnership with other organizations dedicated to the study and enforcement of the LGPD, the TJSC developed an application, called "LGPD-JUS," providing layered authentication of personal data owners, similarly to internet banking applications.

Using blockchain resources, the application – available to all mobile phone systems – provides different levels of access according to the relevance of the data and can operate through low data rate internet connections.

The expectation is that this application will serve as a model to other courts and organizations in Brazil.

Consumer Protection



PROCON-SP and the consumer guidance center

Due to the increase in mobile phone theft and unlawful access to the internet banking applications, the Bureau of Consumer Protection of São Paulo (PROCON-SP) is working to create a consumer guidance center.

Previously, PROCON-SP had already notified ten banks and three financial industry associations to provide clarifications on the operation of data security, blocking and exclusion devices used remotely and requested information on the tracking of financial transactions provided to clients.

Companies operating in the banking and mobile telephone industries have until July 30 to provide details on the measures undertaken when identifying or receiving reports of possible security breaches. In addition, these companies will be required to describe the receipt, handling and storage of personal data provided by data owners, as well as the period of storage and the security policies specifically implemented to address PIX transactions.

In addition, smartphone manufacturers were notified to provide clarifications on the security of their devices. These manufacturers will be required to detail the operation of the system for unlocking and accessing the users' information, as well as on the charges applied for the use of mobile security devices and their respective operational systems, the type of IP registry and storage per user, as well as the security provisions used in remote identification, addressing, location and tracking, in the event of theft/robbery of the device.

Based on the information provided, PROCON-SP intends to provide consumers with the necessary steps to block their accounts and passwords, telephone lines and chips, in a simplified and agile manner, as well as to delete the data stored in their mobile phones in the event of theft and robbery.

SENACON fines financial institutions for the unauthorized use of personal data from elderly users

In a few weeks, the National Consumer Secretariat (SENACON) fined four different financial institutions for the abusive use of personal data from elderly users, specifically with respect to the offer of payroll loans. Fines vary between BRL 4 and 9.6 million.

According to SENACON, these financial institutions violated the provisions set forth in the Consumer Protection Code (CDC) for their non-compliance with the obligation of protection and monitoring of activities carried out by banking representatives, which resulted in the exploitation of elderly users entitled to INSS retirement and pension benefits. In addition to violating the CDC, these financial institutions violated the Brazilian Internet Civil Rights Framework (MCI), which requires the approval of data owners and provides for the right of data owners to exclude their information. Therefore, as stated by the Ministry of Justice, a new proceeding will take place to determine specific violations of the MCI.

Upon receiving reports from the Collective Protection Institute and Brazilian Consumer Protection Institute (IDEC), SENACON verified that consumers whose personal data had been used to offer these kinds of loans were not notified of the disclosure of their data, neither of any registration.

SENACON stated that this matter is a priority. *"We are working on several fronts to prevent these abuses and correct behaviors that jeopardize elderly users,"* stated SENACON secretary, Juliana Domingues, to UOL website.

International Rulings

European national data protection authorities act against two municipalities for violating the General Data Protection Regulation

The first case is connected with the sharing of sensitive personal data, such as information concerning health and other confidential personal data from the data subject's life, before a publishing service, between the Norwegian central and Oslo local governments, called "eInnsyn". When considering the processing a serious violation, the Norwegian National Data Protection Authority fined Municipality of Oslo forty thousand euros.

The document in question was a subpoena, sent by the Oslo's municipal attorney to City Council of Oslo. Norwegian Authority highlighted that the document was not marked as "prohibited from public access", so it was not filed in the internal section, but sent for publication, remaining available to the public for about five hours, before being removed.

In turn, Portuguese National Data Protection Authority (CNPD) understood, after due instruction, that the Municipality of Lisbon, by sharing personal data through communications between the services of the Municipality and with other bodies, violated the General Data Protection Regulation (GDPR).

Portuguese Authority found that the Municipality acted unlawfully and violated the principle of necessity, since GDPR only allows the sharing of information regarding the object, date, time, place, and direction of the communication, without the transmission of any personal data. It is also appointed that the information shared were sensitive personal data, since they contained opinions and religious, political, and philosophical convictions, which required a more careful and responsible processing by the Municipality, as determined by GDPR and Portuguese Constitution, according to Authority.

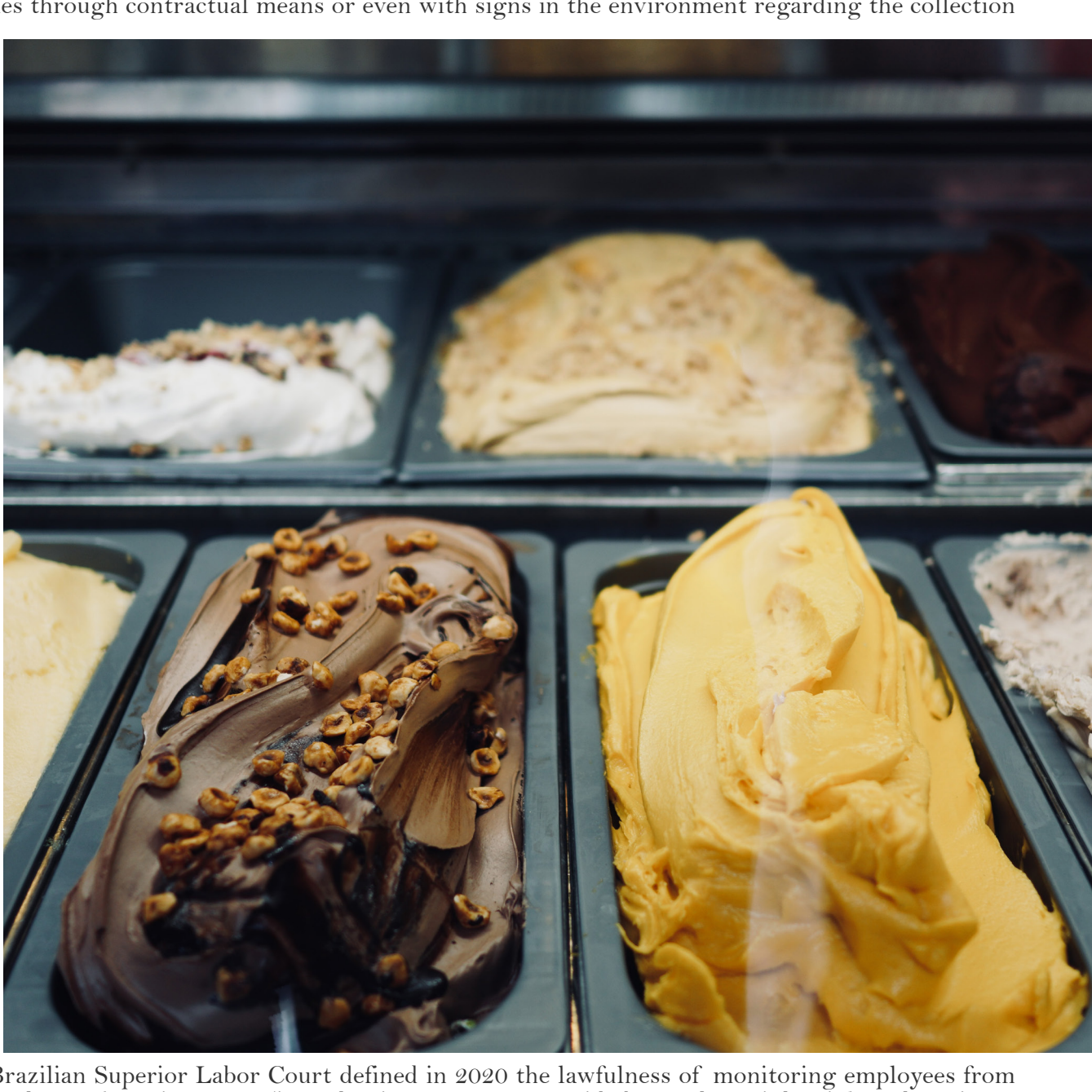
Authority also considered that the sending of personal data by event promoters tends to potentiate illegally the creation of profiles around their ideas, opinions and convictions that is beyond the control of the processing agents, besides putting at risk other fundamental rights provided in Portuguese Constitution. Thus, CNPD has concluded that other violations of GDPR have occurred, such as failure to inform data subjects about the processing of their data.

A deadline is opened for the submission of a defense by the Municipality of Lisbon so that a final decision may be issued by Authority.

Icelandic Data Protection Authority fines ice cream store managing company for improper monitoring of its employees

On June 29, the Icelandic Data Protection Authority fined the company "Huppuís ehf", manager of ice cream parlors, a total of ISK 5,000,000 (approximately R$ 213,000) for violations of the General Data Protection Regulation (GDPR) in the course of the undue monitoring of its employees with surveillance cameras.

As identified by the Authority, Huppuís adopted security cameras in different locations of the company (including the employees' locker rooms), and did not inform them of such monitoring activities through contractual means or even with signs in the environment regarding the collection of data. In this regard, even though the cameras in question were installed for security reasons, the Authority pointed out irregularities as to the scope and the way this monitoring took place.

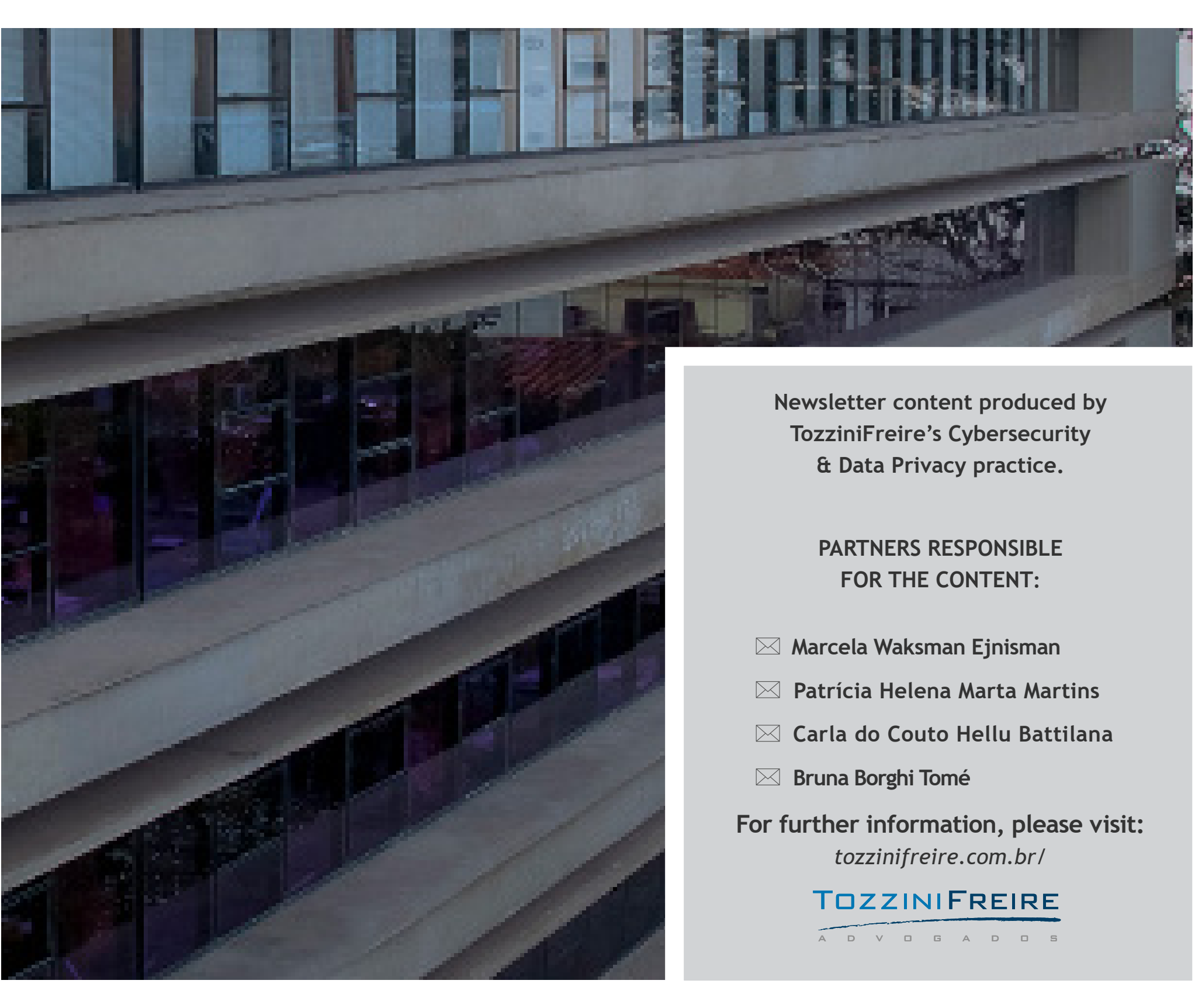


Regarding the scope, the Authority understood that it would not be acceptable for the employees' locker-room to be subject to surveillance by the company. Furthermore, the Authority also concluded that the personal data collected through this system was not processed in a legitimate or transparent manner, nor was it adequate and relevant to meet the purposes that justified its collection. As an aggravating factor in this scenario, several of Huppuís employees are underage individuals, that is, data subjects who receive special protection under data protection regulations.

As a result, the company was forced (i) to stop the monitoring by security cameras of employees wherever they do not exercise their professional activities (such as the locker room), and (ii) to implement procedures that would guarantee access to the employees regarding the necessary information about this operation.

With a similar rationale, the Brazilian General Data Protection Law (LGPD) sets forth as a general principle the need to pursue transparency with the data subjects of the processed data regarding not only the existence of processing activities with their data, but also clear, precise, and easily accessible information about such activities. In addition, the LGPD also establishes the principle of necessity as a guide for an evaluation of what is the smallest amount of data necessary for the pursuit of the specific purpose that guides the processing activity.

In this regard, aligned with such assumptions, the Brazilian Superior Labor Court defined in 2020 the lawfulness of monitoring employees from security cameras, as long as this process is limited to the work environment (i.e., what is necessary to avoid abuses that might violate the privacy of employees as with spy cameras or cameras in bathrooms and locker rooms), also establishing the need to ensure proper transparency with the monitored data subjects (with signs about the monitoring activities, for example).



IMAGENS:CHRISTIAN WIEDIGER, MARKUS SPISKE, SERGEY ZOLKIN, EVGENY TCHEBOTAREV, YIFENG LU, AARON BURDEN, ADITYA JOSHI, JONAS LEE, MIKITA KARASIOU, ERWAN HESRY.

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

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

TOZZINIFREIRE ADVOGADOS