TF cybernews
6th edition | 2021
TozziniFreire Advogados

Brazilian Context

The National Authority publishes its Strategic Plan for the upcoming three years of activities

The National Data Protection Authority (ANPD) published the Strategic Plan for its three upcoming years of activities (from 2021 to 2023), which more clearly defines the macro-objectives that guide its activities, as well as the deadlines for the implementation of each of the Authority's goals.

The Planning also establishes the ANPD's mission, vision, and values. In this regard, the Authority envisions its objective of "ensuring the protection of personal data" (its mission), seeking "to become an example to be pursued, in the national and international levels in the Personal Data Protection scenario" (its vision) and acting, to do so, with "ethics, transparency, integrity, impartiality, efficiency and accountability" (its values).

Based on those guidelines, the three macro strategic objectives that ANPD aims to achieve in the coming years are:

(I) The promotion and strengthening of the personal data protection culture, which involves strategic activities set to prevent and detect any infringements to the Brazilian General Data Protection Law (LGPD). In addition, it includes the development of campaigns regarding that which is set forth in the Personal Data Protection regulation in order to promote the training and guiding of both the society in general and the data processing agents on the matter (thus promoting a more active dialogue with private and governmental institutions);

(II) The establishment of an effective regulatory environment for the personal data protection, which concerns the definition of the Authority's priorities in face of its regulatory agenda, the approval of the specific regulation topics to be later discussed and the establishment of procedures and mechanisms to promptly address identified data breaches and received complaints; and

(III) The improvement of conditions for compliance with data protection normative provisions, which brings together, in turn, the actions aimed at ensuring the adequate and sufficient structure, as well as the physical and budgetary conditions for the proper functioning of the Authority.

In view of this scenario, Planning publicizes the Authority's initiatives and organization, contributing to the creation of a Data Protection environment with greater legal certainty, transparency, and predictability concerning the various unclear issues left in the LGPD for pending specific regulation.

It should be noted that ANPD has a key role in the structuring of a Brazilian data protection culture, as it is responsible for regulating the normative parameters and guidelines on the matter. In addition, the Authority represents an important step towards the greater positioning of the Nation in the increasingly competitive global data protection context.

In face of its regulatory agenda, ANPD starts in January to collect contributions from the civil society on issues related to micro-companies and to the notification of data breaches

On January 29, the National Data Protection Authority (ANPD) started taking in contributions from civil society for the regulation of the specific issues established in the Brazilian General Data Protection Law (LGPD) which it is responsible for.

In particular, ANPD was opened for contributions on the design of the "regulation applicable to (i) micro and small businesses, (ii) incremental or disruptive business initiatives that present themselves as startups or innovation companies, as well as (iii) individuals that process personal data with economic purposes".

Among the issues discussed in this consultation, some specific matters are set forth by ANPD for the receipt of contributions. In this regard, the Authority raised questions on specific issues such as: (i) the criteria that should be considered in the definition of who can be considered a small data processing agent, (ii) the definition of the impacts that the appointment of a Data Protection Officer (DPO) by small agents might cause to their business, as well as (iii) the impacts that the implementation of a LGPD-compliant posture might incur to small data processing agents.

In this process, the Authority accepted contributions until March 1, 2021, during which time ANPD also held meetings with public and private agents involved in the discussion.

It should be noted that differentiated regulation for micro and small businesses is one of the issues set to be regulated in the first phase of the ANPD Regulatory Agenda for the 2021-2022 biennium (published on January 28, under Ordinance No. 11/2021). As a result, the collection of public contributions on the matter (which started in just 1 day after the publication of the aforementioned agenda), denotes the Authority readiness and commitment towards the implementation of its schedule of activities.

In a parallel discussion, ANPD has also initiated a process of seeking for contributions on the scope of the data breach notification scenario (pursuant to the LGPD's Article 48). Please note that the contributions must follow a specific structure published on the ANPD website and can be sent from February 22 to March 24, 2021 (access here).

ANPD has already made available a personal data breach incident reporting form, as well as a guidance document in case of data breaches, which will serve as guidelines for data controllers as long as there is no specific regulation from the Authority in this regard (access here).

These initiatives are aligned with the ANPD's regulatory expectation, which set the beginning of the personal data breach scenario regulation (in particular, the notification of such breaches and the deadlines to do so) in its Regulatory Agenda for 2021.

Brazilian National Data Protection Authority calls candidates for the formation of Brazilian Data Protection Council

Earlier this month, the Brazilian National Data Protection Authority (ANPD) published the Public Notices for the formation of a triple list for the composition of Brazilian Data and Privacy Protection Council (CNPD). Formed by 23 (twenty-three) regular members and meeting ordinarily 3 (three) times a year, CNPD will take responsibility for: (i) proposing strategic guidelines and providing contributions for the elaboration of Brazilian National Personal Data Protection Policy; (ii) preparing annual reports evaluating the implementation of National Policy actions; (iii) suggesting actions to be taken by ANPD; (iv) preparing studies and promoting debates and public hearings on the privacy and personal data protection matters; and (v) disseminating knowledge about data protection and privacy issues to the population.

Through the Public Notices, ANPD called on civil organizations working in personal data protection matters, scientific, technological and innovation institutions, as well as Trade Union Confederations representing the economic categories of the productive sector, in order to indicate the names that should be included in a triple list that will fill 3 (three) vacant positions in CNPD.

In turn, the business sector entities related to the personal data processing matter and the labor sector entities were also called to indicate names for the formation of a triple list to fill 2 (two) vacancies in Brazilian Council.

Additionally, the definition of the names for the triple list will be made based on specific criteria such as representativeness and experience of the candidate in the personal data protection area. It should be noted that all positions have a two-year term, being only one reappointment permitted, for the same period.

Judicial Branch

Sigilo Institute files a class action against Serasa Experian due to the "super leakage" of data

Despite of the administrative investigations in progress filed by SENACON and PROCON-SP with respect to the company responsible for the "super leakage" of the personal data that affected over 220 million Brazilians, the Brazilian Personal Data Protection Institute (Sigilo Institute) filed a civil lawsuit against Serasa Experian.

In the lawsuit, Sigilo Institute alleged that Serasa Experian is responsible for the "super leakage" of data and requested the payment for collective moral damages in the amount of R$ 200 million, in addition to the indemnity in the amount of R$ 15,000 for each of the data owners affected by the leakage. Added to the indemnity requests, Sigilo Institute requested Serasa Experian to individually inform, through letter with confirmation of receipt, all data owners affected by the leakage, as well as disclose the information regarding which security incidents ocurred and the measures to be adopted to (i) remove such data from the Internet; (ii) stop the damages against the data owners; and (iii) resolve the possible and future risks against the consumers.

Sigilo Institute also included, as defendant, the Federal Government, represented by ANPD, based on the supposed omission of ANPD and also requested the notification of Serasa Experian to conduct the technical audit to determine the security failure related to the incident, including the notification of the personal data owners with respect to such leakage.

After notification of the Federal Government, the request for a preliminary injunction is pending decision.

Data involving 11 Ministers of STF is available for sale after the larger leakage ever registered in Brazil

In relation to the "mega leakage", the data of some Brazilian authorities is available for sale in the Internet, including the data involving 11 Ministers of STF.

As requested by *O Estado de S. Paulo* newspaper, a security company verified that the data offered by the person responsible for the leakage is divided in 37 categories, and that the data of all Ministers of STF is available in more than 20 categories. According to the material published, the data would be sold in packages, at the initial price of US$ 500, considering that 10 is the maximum limit of data categories that could be purchased using the same CPF (Brazilian Natural Person Registry) number.

The "basic" category, which includes CPF number, full name, sex, gender, and date of birth, was the sole category that was fully published and that covered the highest number of persons; it is not possible to confirm whether the persons responsible for the data leakage have indeed all information offered.

After disclosure of information, the president of STF, Luiz Fux, submitted notices to the Minister of Justice, André Mendonça, and Minister Alexandre de Moraes, Reporting Minister of the Inquiry No. 4,781 (Fake News Inquiry) and requested the adoption of applicable measures. In this regard, Minister Alexandre Moraes determined that the Federal Police should open the police investigation to verify the issue, taking into account that such incident affects directly the privacy, intimacy and security of the Ministers. In addition, Minister Alexandre Moraes requested that the report prepared by the expert is submitted to STF and, by prevention, the issue shall be conducted under the responsibility of such Minister.

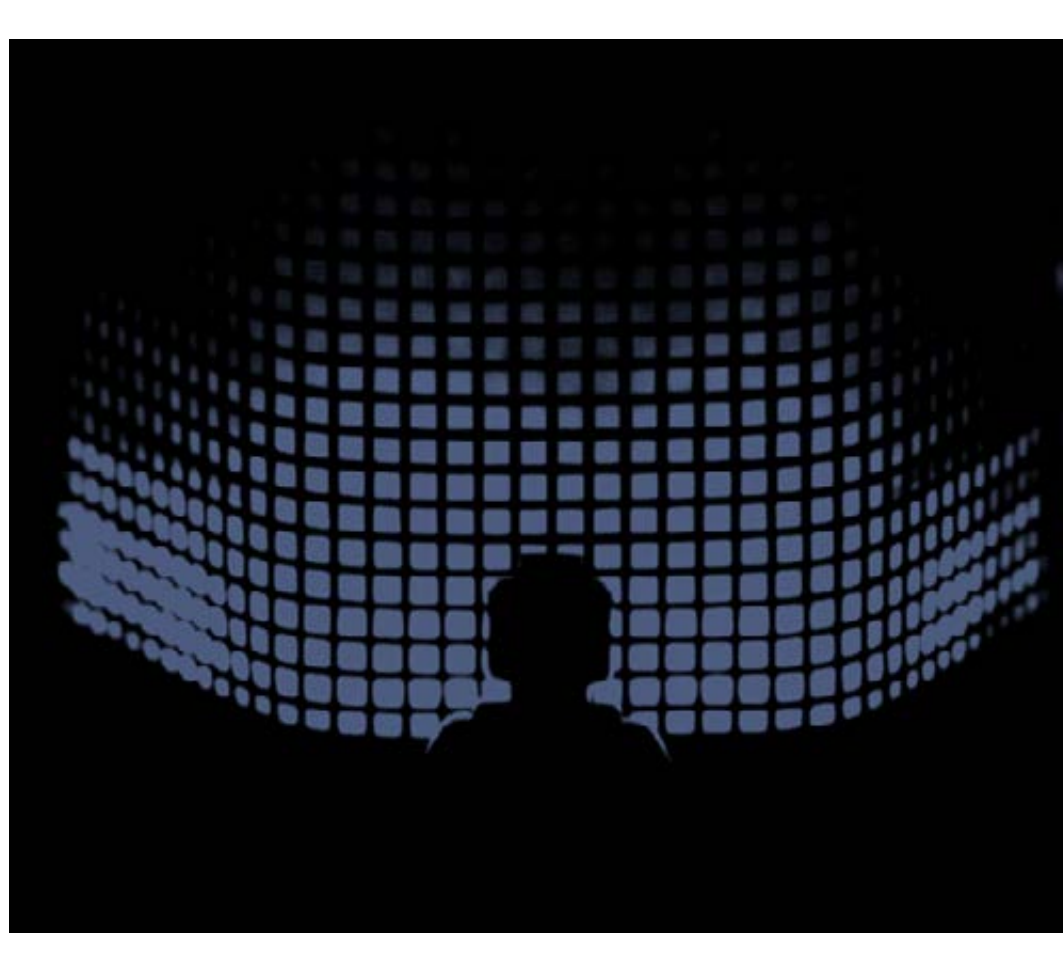
Ombudsman is in charge of the personal data protection under the Superior Electoral Court

On January 12, 2021, the Superior Electoral Court (TSE) published Ordinance No. 14/2021, which designated the unit in charge of the personal data protection under TSE. The Ombudsman of the TSE is the body responsible for the receipt of the claims and doubts submitted by the persons whose data was addressed by TSE.

As set forth in article 5, item VIII, of LGPD (Brazilian General Protection Act), the person in charge is that one designated to "act as the communication channel between the controller, the data owners and the National Data Protection Authority (ANPD)". Furthermore, article 41, paragraph 2, of such Law, defines the duties attributed to the responsible person, who shall adopt the measures in relation to the claims submitted by the data owners and the communications with ANPD, as well as direct the body's employees with respect to the measures to be adopted for personal data protection. However, as set forth in paragraph 3 of such Law, ANPD may define supplementary rules with respect to the duties attributed to the responsible person.

According to the information published by TSE, the notices on the personal data handling shall be submitted directly to the Ombudsman through the reporting channels, including telephone call or completion of the electronic form, which requests the provision of the following information: name, age, state, and email.

Consumer Protection



Administrative investigations began to identify the origin of the "super leakage" of data

In view of the "super leakage" of data that revealed personal information, such as name, CPF (Brazilian Natural Person Registry) number, picture, income and other financial information, individual income tax, information on schooling, marital status, credit scores, and addresses of over 220 million Brazilians, the administrative authorities responsible for consumer protection began the investigations to identify the origin of the incident:

- SENACON (National Consumer Secretariat) notified Serasa Experian to request explanations with respect to the potential involvement of Serasa Experian in the incident and what type of data would have been improperly disclosed, to whom and for how long, as well as whether Serasa Experian has adopted measures to improve the security of the data owners;
- PROCON-SP (Department of Consumer Protection and Defense in São Paulo) also notified Serasa Experian and requested clarifications on the potential involvement of Serasa Experian in the data leakage, the motives that caused the problem, the measures adopted to stop the problem, as well as the actions undertaken to recover the damages and prevent the repetition of such an event.
- ANPD (National Data Protection Authority) declared that the technical information on the incident is being analyzed and ANPD shall cooperate with the proper investigation bodies to understand the origin of the data leakage, how the data leakage took place, the measures adopted for resolution and mitigation in the contingency plan, as well as the possible effects.
- MPF-SP (Federal Public Ministry in São Paulo) confirmed the receipt of at least one formal request for investigation of the incident.
- MPDFT (Public Ministry of Federal District and Territories) has been analyzing the incident and, as of the date hereof, MPDFT shall not comment on the incident.

In response to the notice submitted by PROCON-SP, Serasa Experian informed that the company complies with the provisions set forth in the General Data Protection Law with respect to all and any transactions involving personal data and implemented the information security, and training program to the company's employees.

Additionally, Serasa Experian mentioned that a detailed investigation is under progress; however, as of the date hereof, the company was not able to identify any evidence of invasion in the systems or otherwise that the positive or negative credit data were unlawfully disclosed.

According to the executive officer of PROCON-SP, Fernando Capez, the information provided by Serasa Experian was generic and insufficient, without any description of the technical and organizational measures adopted by the company, based on which Fernando Capez would not disregard the internal leakage and the absence of legal basis for the treatment and use of personal data without any restrictions.

PROCON-SP does not disregard the possible application of the fine set forth in the Consumer Protection Code – which may reach the amount of R$ 10 million – after the conclusion of the analysis of the information provided by Serasa Experian.

2021 SENACON agenda regarding data protection and strengthening of relations with ANPD

The National Consumer Secretariat (SENACON) along with the National Data Protection Authority (ANPD) have promoted an institutional strengthening of relations to address the personal data protection.

In this regard, SENACON created a Group under the National Council for Consumer Protection (CNDC) to promote the direct contact with ANPD for the development of joint activities relating to the personal data protection in the context of the consumer relations – which would ensure, therefore, both the consumer protection and the personal data security. Accordingly, lawyers Laura Schertel Mendes and Luciano Timm, experts in consumer protection, shall support the CNDC.

The Technical Cooperation Agreement (ACT) is also expected to be entered into in March for purposes of protection of the consumer's data, in relation to which SENACON intends to share the collected information on the consumers' claims with respect to personal data protection, while ANPD shall present the necessary interpretation for the application of the LGPD in concrete cases. The purpose is to align various interpretations to carry out the implementation of a coordinated action plan to address the consumers' claims.

At the meeting held with the National Consumer Secretary, Juliana Oliveira Domingues, the president of ANPD, Waldemar Gonçalves, stated that the partnership between the authorities is very positive, considering that such partnership shall define the specific role of each authority in terms of data protection in Brazil.

Furthermore, in recent interviews, the National Consumer Secretary informed that SENACON has already received 42 requests for administrative investigations involving data protection, in addition to the increased number of cases that involve significant leakage of the consumers' data, including the verification of evidence and authorship of these incidents, subject to the application of the sanctions set forth in the Consumer Protection Code (CDC).

The Secretary has also been considering the activities of the big techs, specifically by virtue of economic power, in order to avoid the unlawful exposure of the consumers' personal data through data sharing and directed marketing, and also emphasized that the issue requires the technical analysis and proper application of the CDC's provisions to the new technological scenarios.

PROCON-SP requests the opening of a police investigation and STF determines the suspension of the website "fuivazado.com.br" in the context of the Fake News Inquiry

PROCON-SP submitted the request for the opening of a police investigation to the General Head of the Police of the State of São Paulo for the investigation of the activities of the website "fuivazado.com.br", which offers the confirmation – by means of consultation of the CPF (Brazilian Natural Person Registry) or CNPJ (Brazilian National Registry of Legal Entities) number and date of birth – whether the users were affected by the "super leakage" of personal data of over 220 million Brazilians at the beginning of the year.

According to PROCON-SP, the website accessed over 223 million CPFs and over 40 million CNPJs included in lists that were unlawfully available on the Internet, in addition to the donations in cash from the users to maintain the website's activities.

However, according to PROCON-SP, the website (i) did not clarify the need or the purposes of the users' personal data in the consultation, as well as (ii) did not inform how the lists including the personal data were obtained.

The investigation conducted by PROCON-SP shall verify the possible violation of the personal data protection legislation in force, as well as the possible unlawful commercial activities by the website.

Concurrently, the website "fuivazado.com.br" was suspended after the determination of the Minister of the Federal Supreme Court (STF), Alexandre de Moraes, in the context of Inquiry No. 4,781, known as Fake News Inquiry.According to the Minister, more than informing the users about the data leakage, the website would have unlawfully sold the personal data of national authorities and Ministers of the STF.

Accordingly, the Minister determined the hearing of the person identified as the responsible for the website and the immediate removal from the companies' results of the reference to such website. Since then, the website is unavailable.

International Rulings

European Data Protection Board Guidelines on examples regarding Data Breach Notification

On January 14, 2021, the European Data Protection Board (EDPB) issued "Guidelines 01/2021" regarding personal data breach notification. These guidelines were issued in order to complement the general guidance issued by the Working Party Article 29, based on the European experience with the entry into force of European General Data Protection Regulation (GDPR). Its objective is to help data controllers to deal with data breaches, informing the factors that should be considered when assessing the risks involved in the breach.

EDPB reiterates that, when attempting to address a breach, the controller must first be able to identify one. In this regard, the data breaches can be classified in three categories: (i) "Confidentiality breach", in which there is an unauthorized access or accidental disclosure of personal data, (ii) "Integrity breach", when there is an unauthorized or accidental change of personal data, and (iii) "Availability breach", in which there is a loss or destruction of personal data.

A data breach can potentially have a series of adverse effects on individuals, which can result in physical, material or psychological damage. GDPR establishes that such damages may include the loss of control over the data subjects' personal data, the limitation of their rights, as well as scenarios of discrimination, fraud, financial loss, unauthorized reversal of pseudonymization, reputational damage and loss of confidentiality about data protected by professional secrecy. For this reason, EDPB emphasizes that one of the most important obligations of the controller is to assess such risks on the data subjects' rights, which should be done in parallel with the implementation of the appropriate technical and organizational measures to address them.

In this regard, the European regulation requires the agent to keep records of any personal data breaches, their effects, and the corrective measures adopted to resolve them. In addition, the data controllers are entitled to the obligation of notifying the occurrence of a personal data breach for both the National Authority and the affected data subjects (for those individuals, however, only when there is a likelihood of resulting in a high risk to their fundamental rights).

Pursuant to that which is set forth in the Guidelines, the data breaches are symptoms of a vulnerable and outdated security regime, which indicates deficiencies that should be addressed. Before a controller can fully assess the risk from a data breach, the cause of the problem must be identified. In this regard, it is also necessary to verify whether the vulnerabilities that led to the incident are still present in the controller´s systems. In many cases, the data processing agent is able to identify whether or not the data breach may result in a risk and therefore notify it, yet exceptions may occur. It is recommended, therefore, that the notification be not postponed until the beach´s impact has been fully assessed, after all, the complete assessment might still be made in a complementary future notification.

It should be noted that the breach must be notified whenever the data processing agent considers that it is likely to result in a risk to the data subject's rights, being such assessment necessary at the moment that they become aware of the breach. The guidelines are clear about the fact that the agents should not wait for a detailed examination of the matter or even for the adoption of the first steps to mitigate the risks so that only then the notification is sent.

As recommended by EDPB, each agent must have plans to address with any personal data breaches. It is essential, therefore, for their due preparation on data protection issues (especially when it comes to handling data breaches). It is recommended, therefore, that trainings be regularly conducted, discussing the latest highlights on the data breaches matter.

EDPB also recommends that each organization should structure guidelines (prior to the existence of a breach) that would work as a quick source of information to allow agents to mitigate risks without delay. In this regard, should personal data breach take place, the guidelines would ensure that the data processing agents' personnel would know how to address the breach, dealing with it with greater efficiency. Finally, the Guidelines define that keeping records of data breaches is an independent obligation that arises from the inherent risks in the breach, which should be carried out whenever a data breach takes place.

Facial Recognition: data subjects' faces taken as barcodes

The Dutch Data Protection Authority issued a formal warning to a supermarket due to the use of facial recognition technology. Even though the same technology had already been previously disabled, the supermarket intended to use it again.

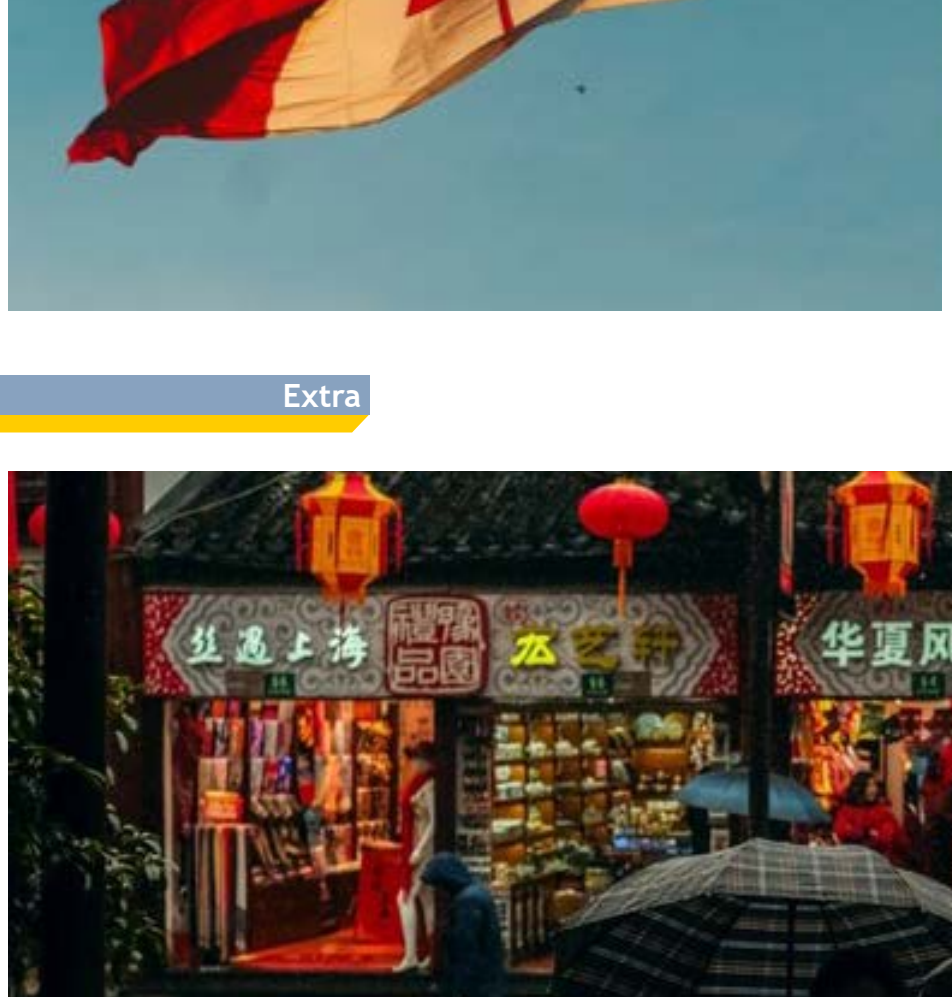
To do so, the supermarket argues that such facial recognition system should be used for the protection of customers and employees, as well as theft prevention. The technology, linked to the supermarket's entrance cameras, scanned the faces of individuals who entered in the store and compared such images to the database of individuals who had been previously banned from the supermarket.

The deputy chairperson of the Dutch Data Protection Authority, when commenting on the case, said that it would be unacceptable the use of facial recognition technology by the supermarket, as well as by any other store in the Netherlands. She signaled that facial recognition turns individuals into "walking bar codes", pointing out as well the fact that such technology was being used without the data subjects' prior consent. In addition, to the deputy chairperson mentioned that the facial recognition technology exposes individuals' faces in a search engine that is capable of relating these images to their names as well as to any other personal data, including those available on social networks.

In the Netherlands, given that the facial technology mechanism functions with the usage of biometric data, the Dutch Data Protection Authority establishes that it is only allowed in two specific scenarios: (i) when there is explicit consent from the data subject; or (ii) when the technology is necessary for authentication or for security purposes insofar as there is a public interest involved, as in the security of a nuclear power plant, for instance.

In the Brazilian context, it is should be noted tha facial recognition has already been subject of discussions. In early 2019, a wanted man by the police was arrested after having his face recognized by a facial recognition camera at the Carnival in Salvador. In the same year, in Rio de Janeiro, a woman was mistakenly detained because of a failure in the Military Police's facial recognition system. Additionally, at the beginning of last year, the São Paulo Court of Justice determined that the São Paulo Metro should provide explanations about the facial recognition project by cameras and the data processing to be carried out by this technology.

American facial recognition company illicitly carries out mass surveillance in Canada



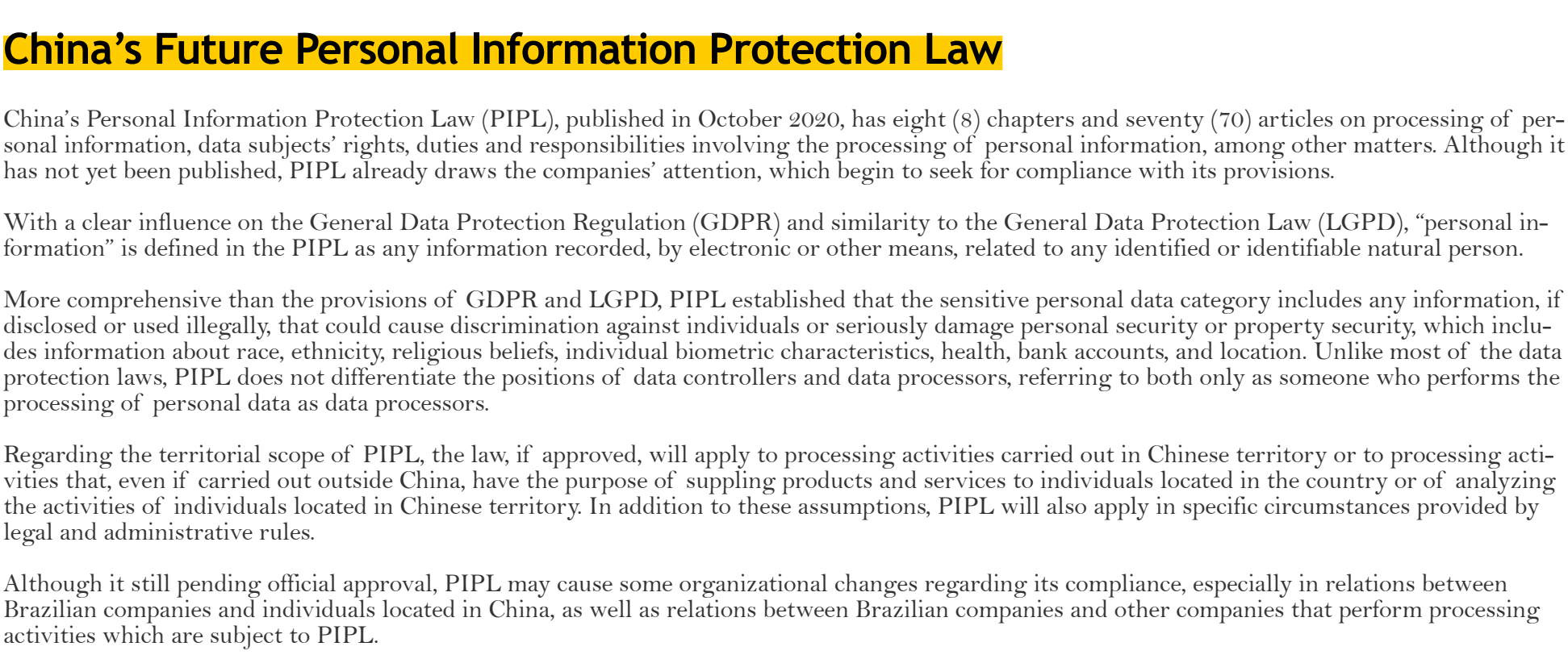
The Clearview AI (a facial recognition company) allowed, through its services, for the police and commercial organizations to combine photos of unknown individuals with its database of more than three billions images (with Canadians and children data), for investigative purposes.

In an investigation carried out by the Canadian Data Protection Authority, it was found that this software allowed the potential creation of significant damage to individuals, who have never been involved in crimes and whose photos were collected, disseminated and disclosed by Clearview AI. The Canadian Authority understood that there was a collection of highly sensitive biometric data without any knowledge or prior consent from its data subjects.

Although Clearview AI claims that Canadian privacy laws do not apply to its activities (as there is no direct relation between the company and Canada), it states that the data subjects consent was not necessary (especially considering that the information collected was publicly available). The Canadian Authority rejected these and other arguments from the company, which stopped providing its services in the Canadian market at the beginning of the investigation.

In the Brazilian scenario, even if data processing does not take place in Brazilian territory or if the processing agents – controllers and operators – are not located in Brazil, the Brazilian General Data Protection Law ("LGPD") is applicable, due to its extraterritorial scope. Thus, if personal data, including images, have been collected in Brazil or if the processing activity has by purpose the processing of personal data from individuals located in the national territory – such as the surveillance of individuals who are in Brazil – LGPD indeed will be applicable.

Extra



China's Future Personal Information Protection Law

China's Personal Information Protection Law (PIPL), published in October 2020, has eight (8) chapters and seventy (70) articles on processing of personal information, data subjects' rights, duties and responsibilities involving the processing of personal information, among other matters. Although it has not yet been published, PIPL already draws the companies' attention, which begin to seek for compliance with its provisions.

With a clear influence on the General Data Protection Regulation (GDPR) and similarity to the General Data Protection Law (LGPD), "personal information" is defined in the PIPL as any information recorded, by electronic or other means, related to any identified or identifiable natural person.

More comprehensive than the provisions of GDPR and LGPD, PIPL established that the sensitive personal data category includes any information, if disclosed or used illegally, that could cause discrimination against individuals or seriously damage personal security or property security, which includes information about race, ethnicity, religious beliefs, individual biometric characteristics, health, bank accounts, and location. Unlike most of the data protection laws, PIPL does not differentiate the positions of data controllers and data processors, referring to both only as someone who performs the processing of personal data as data processors.

Regarding the territorial scope of PIPL, the law, if approved, will apply to processing activities carried out in Chinese territory or to processing activities that, even if carried out outside China, have the purpose of suppling products and services to individuals located in the country or of analyzing the activities of individuals located in Chinese territory. In addition to these assumptions, PIPL will also apply in specific circumstances provided by legal and administrative rules.

Although it still pending official approval, PIPL may cause some organizational changes regarding its compliance, especially in relations between Brazilian companies and individuals located in China, as well as relations between Brazilian companies and other companies that perform processing activities which are subject to PIPL.

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

PARTNERS RESPONSIBLE FOR THE CONTENT:

Marcela Waksman Ejnisman
Bruna Borghi Tomé
Carla do Couto Hellu Battilana
Patrícia Helena Marta Martins

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

TozziniFreire Advogados

IMAGENS: UNSPLASH