

DATA PROTECTION & LITIGATION

The leading role of public bodies in privacy and data protection: history, fines, and agreements in Brazil

ARTICLE 3

THE LEADING ROLE OF PUBLIC BODIES IN PRIVACY AND DATA PROTECTION: HISTORY, FINES, AND AGREEMENTS IN BRAZIL

In the last article of the series, we went through the path of publication of the General Data Protection Act (Law No. 13,709/2018 – “LGPD”) in Brazil, covering the legislative path until the law becomes fully effective, and the subsequent entry into force of administrative sanctions in August 2021. The article also brought a heated discussion about the retroactivity of the application of LGPD sanctions. To remember, click [here](#). Precisely in the context of the application of sanctions, the theme of our 3rd article arises.

This is because, despite privacy and data protection gaining greater media coverage in 2020, also driven by the engines of the COVID-19 pandemic – which launched and/or implemented numerous health technologies based on the processing of personal data – the subject matter is not new in our legal system, especially for some bodies such as consumer protection and the Prosecution Office of the States, which were already working on the matter, notifying, investigating, entering into agreements or terms of conduct adjustment and, even imposing sanctions on several companies for violations of privacy and data protection.

Although there was no specific law on the subject matter published or fully in force, the legal system already provided numerous useful instruments for the aforementioned action. The [Brazilian Constitution of 1988](#) (“CF/88”) already provided, in its article 5, item X, for the inviolability of people's private life, honor and image. Nonconstitutional laws also already address the subject matter, placing privacy and data protection as guiding principles, such as the [Civil Rights Framework for the Internet](#) (Law No. 12,965/2014) and its [Regulatory Decree](#) (Decree No. 8,771/2016), in addition to the [Consumer Protection Code](#) itself (Law 8,078/1990), which provides for the need for transparency in the processing of personal data of consumers. And these were laws that, for the most part, substantiated the performance of the public bodies.

The Prosecution Office of the Federal District and Territories (“MPDFT”) proved to be a pioneer in terms of privacy and data protection. In 2017, the body created, within the scope of the Prosecution Office for Consumer Protection, the Commission for the Protection of Personal Data. Then, in January 2018, MPDFT worked in the case of the data breach of [Netshoes](#), which involved the alleged leak of more than two (2) million personal data, including data from politically exposed public officers. The MPDFT, through [Recommendation No. 01](#) of 2018, indicated that the company should: (i) notify the affected data subjects, through correspondence and telephone calls, and (ii) refrain from making payments to the Hacker.

In April 2018, MPDFT created the [Special Unit of Data Protection and Artificial Intelligence](#) (“ESPEC”), through [Normative Ordinance No. 539](#), of April 12, 2018. In the same month, and demonstrating the body's leading role, the MPDFT entered into an agreement with the company [Uber](#), due to the data breach that would have exposed fifty-seven (57) million accounts of drivers and customers from several countries. In that act, the company committed to notifying the more than one hundred and ninety-six (196) thousand Brazilian users affected, publicizing the infraction, with a position very similar to the case involving Netshoes.

Shortly thereafter, in July 2018, the Department of Consumer Protection and Defense (“DPDC”), a body of the Ministry of Justice, ordered the company [Decolar.com](#) to the payment of a fine of seven million and five hundred thousand reais (BRL 7,500,000.00) for arguing that there would be a differentiation in accommodation prices and a refusal to offer vacancies according to the customer's geographic location (geo pricing and geoblocking, respectively). Although the decision did not expressly mention privacy or data protection, it was based on the abusive, discriminatory processing of personal data and the breach of the legitimate expectation of the data subject/customer, for the application of the penalty.

The scenario did not change with the enactment of the LGPD in August 2018. A few months later, after filing a Public Civil Action, MPDFT ratified an agreement with a financial institution as a result of the leak of data from more than nineteen (19) thousand account holders, in which the institution disbursed the amount of one million and five hundred thousand reais (BRL 1,500,000.00), as a way of repairing national collective moral damages.

In February 2019, and concluding the subject matter with Netshoes, the MPDFT entered into a [Conduct Adjustment Agreement](#) (TAC), providing for the indemnification of five hundred thousand reais (500,000.00) to the Fund for the Defense of Diffuse Rights as compensation for the collective moral damages caused. The company also committed to implementing additional measures to its Data Protection Program, with the continuous updating of its Cyber Security Policy; using efforts to guide consumers, through an awareness campaign; and disseminating best practices for privacy data protection in the market, through participation in specialized forums and events.

In April of the same year, the MPDFT issued a ministerial order in the record of the [Public Civil Investigation No. 08190.005366/18-16](#), requesting a Data Processing Impact Assessment (“DPIA”) from the company Telefônica, as a result of the data processing used in the Geolocated Media product of the Vivo Ads service, a platform used by the company to track the geolocation of its users. The referred order was extremely criticized for requiring conduct not yet in force in law, nor regulated (at the time, the articles referring to the DPIA were still in [vacatio legis](#)).

But it was not just that. The case was still the object of a Public Civil Action^[1] filed by the MPDFT. However, the judgment denied the claims of the ministerial entity, observing the impossibility of requesting a DPIA, since the issue was still pending regulation by the Brazilian Data Protection Authority (“ANPD”). The decision of the trial court was confirmed in the appellate decision, because the company “(...) at the time of contracting, allows the consumer to express their consent or disagreement in receiving “offers and benefits” from Vivo and its Partners, through the use of their “personal and location data”, in addition to having a Privacy Center available to the subjects, and the lack of evidence from the MPDFT on the dissatisfaction or injury of the customers/ data subjects was verified.

In August 2019, although the provisions related to the sanctions provided for in the LGPD were not yet in force, a severe pecuniary fine was imposed, based on the principles provided for in that rule. Procon Foundation (Program for the Consumer Protection and Defense) of São Paulo imposed fines on [Google](#) and [Apple](#) of, respectively, nine million and nine hundred thousand reais (BRL 9,900,000.00) and seven million and seven hundred thousand reais (BRL 7,700,000.00) due to the violation, by the companies, of the Consumer Protection Code, for making the “Face App” application available in their stores, which performed the aging process of faces in photographs. The fines would have been based, among other particularities, on the fact that the Privacy Policy and the Terms of Use would be in the English language (impairing the transparency of the document, which would not have been provided in the Portuguese language) and that the companies would have abusive clauses in their policies and terms, concerning to the sharing and data transfer, in addition to the alleged absence of an opposition mechanism available to the data subject.

Later, in December 2019, the Consumer National Department of the Ministry of Justice (“Senacon”) fined [Facebook](#) six million and six hundred thousand reais (BRL 6,600,000.00), for sharing personal data in the case of Cambridge Analytica, known worldwide, in which data from millions of users would have been used by the digital marketing company to influence political choices. Senacon applied the fine for understanding that the company acted in an abusive way, not correctly communicating with its users about its privacy practices.

In April 2020, for household surveys via telephone, to maintain the continuity of surveys, during the pandemic, such as the PNAD - Continuous National Household Sample Survey - determined by Provisional Measure No. 954/2020 (“MP”), fixed and mobile telephony operators were compelled to transfer their customer registration to the Brazilian Institute of Geography and Statistics (“IBGE”).

[1] Public Civil Action No. 0721735-15.2019.8.07.0001. Reporting Judge José Divino. Appellate Decision published on 06/05/2020. Available at: [Lawsuit Detail · Electronic Judicial Process - Court of Appeals \(tjdf.jus.br\)](#)

In response to the MP, the Council of the Brazilian Bar Association (“OAB”) and Political Parties filed five Direct Actions of Unconstitutionality (“ADIs”), because the MP's object violated people's privacy, private life, and confidentiality of data. In a historic decision, the [Federal Supreme Court suspended the effectiveness of the MP\[2\]](#), under the main argument of application of the principle of reasonableness and proportionality, not allowing the Brazilian justice to make an exception in the face of a health crisis and, with that, remove fundamental civil rights and liberties.

Still in the field of the health crisis caused by COVID-19, Procon of São Paulo, in November 2020 and based on the LGPD, notified [Hospital Albert Einstein](#) requesting explanations about the alleged leak of lists with personal and medical information of patients tested, diagnosed, and hospitalized for COVID-19. In addition, Procon also requested clarification on which information security measures were adopted as a result of the data breach.

Thus, the year 2020 came to an end with numerous cases in progress; in November of that year, the ANPD began its activities, with the [appointment of the Board of Directors](#) and, in December, with the publication of the [regulatory structure of the Authority](#). And, since then, the ANPD has been in a growing, solid, and extremely relevant operation for the privacy and data protection scenario in Brazil, focused, at this first moment, on issuing regulations and operational guides.

This is what was seen at the beginning of 2021, with the publication, by the ANPD, of its Regulatory Agenda ([Ordinance No. 11 of January 27, 2021](#)). Among the works, [CD/ANPD Resolution No. 1 of October 28, 2021](#) was published, which approved the [Regulation of the Inspection Process and the Sanctioning Administrative Process within the scope of the ANPD](#), embodying the procedure whose objective is the investigation and eventual application of sanctions in the regulatory scope. It is a fact that, under the terms of article 71 of the Regulation, there is a provision for the issuance of an Ordinance with additional instructions on the inspection and sanctioning process, but the activity may start at any time, opportunity in which the cases will also proceed in the specific body, and not only in those related to consumer protection, the Prosecution Office, or submitted to the Judiciary Branch.

[And the action of the ANPD has already taken place](#). In October 2021, the ANPD started the investigation of the case of information leakage through the Instant Payments System (“Pix”), a case that is being proceeded under legal confidentiality, due to the industrial and commercial secrets contained in the investigation.

[2] Direct Action of Unconstitutionality (“ADI”) No. 6388. Reporting Judge Rosa Weber. Decision published on 05/07/2020. Available at: [Federal Supreme Court \(stf.jus.br\)](#)

Direct Action of Unconstitutionality (“ADI”) No. 6389. Reporting Judge Rosa Weber. Decision published on 05/07/2020. Available at: [Federal Supreme Court \(stf.jus.br\)](#)

Direct Action of Unconstitutionality (“ADI”) No. 6390. Reporting Judge Rosa Weber. Decision published on 05/07/2020. Available at: [Federal Supreme Court \(stf.jus.br\)](#)

Direct Action of Unconstitutionality (“ADI”) No. 6387. Reporting Judge Rosa Weber. Decision published on 05/07/2020. Available at: [Federal Supreme Court \(stf.jus.br\)](#)

Direct Action of Unconstitutionality (“ADI”) No. 6393. Reporting Judge Rosa Weber. Decision published on 05/07/2020. Available at: [Federal Supreme Court \(stf.jus.br\)](#)

Subsequently, the ANPD also started the investigation of the incident involving the [Ministry of Health and Conecte SUS](#), notifying them to provide clarification, considering the sensitivity of the case and possible serious damage to the data subjects involved. These are just two (2) public cases to which people have access, but it is estimated that countless others are probably already in progress.

But do not misunderstand. In a country where judicialization rates are very high (such as consumer cases), and with numerous consumer protection bodies (which are not criticized, it is only observed), it is quite likely that the investigation of data breaches or improper processing of personal data does not fall solely and exclusively into the hands of the ANPD.

It is worth mentioning that, despite the LGPD granting exclusivity to the application of its administrative sanctions to the ANPD, with the prevalence of its competencies over other entities and bodies, the administrative bodies have continued to act on the subject matter, especially because of the inexorability of other legal provisions. This is the case, for example, of Senacon, which in June 2021 fined [Banco Cetelem S.A.](#) four million reais (BRL 4,000,000.00) under the allegation of abusive offer and contracting of automatic-paycheck-deduction loans with the improper use of personal data of elderly consumers. In August of the same year, Procon of Mato Grosso fined [Raia Drogasil Group](#) in the amount of five hundred and seventy-two thousand reais (BRL 572,000.00), under the allegation of irregular use of sensitive personal data of biometrics and lack of transparency with customers about its practices.

Thus, given the history and how much has been discussed so far, the constant and frequent action of public bodies concerning privacy and data protection is evident, even before the partial or full validity of the LGPD or the structuring of the ANPD.

Regarding the ANPD, the expectation is that, in the coming months, its performance will become even more relevant, with the beginning of the application of the administrative sanctions of the LGPD. It is time to prepare for what will come, in a scenario where judicial decisions, agreements, fines, conduct adjustment agreements, and sanctions applied by the ANPD can coexist. We look forward to the next chapters of this story.

AUTHORS



 Danielle Cavalcante
dcavalcante@azevedosette.com.br



 Lorena Pretti Serraglio
lserraglio@azevedosette.com.br



 Camilla Chicaroni
cchicaroni@azevedosette.com.br