

Data Protection:

overview on sanctions around the world and forecast of ANPD fines from February



By: Daniela Machado e Míriam Ferreira
Layout: Anaís Moura
Coordination: Clarissa Luz
Privacy, Data Protection and Technology Team:
privacy@felsberg.com.br

20
23

INTRODUCTION

February, joy, carnival and... sanctions from the ANPD? In several events that took place in the last week of the (long) month of January, the president of the Brazilian National Data Protection Authority (ANPD), Waldemar Gonçalves, stated that the preparation of the "Regulation on Dosimetry and Application of Administrative Sanctions" is in its final stages, and should be approved up to the end of February.

And what does this mean for companies, given that the Brazilian General Personal Data Protection Law (LGPD) has been in force since September 18, 2020?



It means that, in addition to the sanctions that are already being applied by the Judiciary - in individual and collective litigation - and by the National Consumer Defense System's bodies, such as the National Consumer Secretariat (Senacon) and the Procons, the ANPD will very soon begin to apply sanctions to companies that process personal data.

This is, therefore, a fundamental step on the path to achieving the full effectiveness of the LGPD and the establishment of a culture that contemplates the protection of personal data in Brazil. By clearly defining the parameters and methodology for applying the sanctions provided for in Article 52 and respective sections of the LGPD, the ANPD ensures greater legal certainty for processing agents, since it allows greater predictability about the consequences of unlawful acts.



The topic was the subject of a public consultation initiated in August 2022, which received **2.504** contributions from entities and members of civil society, companies and professionals in the area. It is expected that, with the publication of the regulation, the ANPD will act in a more incisive manner in the inspection and sanctioning of processing agents, starting with **8** cases with pending decisions by the authority, as mentioned by Waldemar Gonçalves.

It should be noted that the [Regulation of the Inspection Process and the Sanctioning Administrative Process](#) was approved by Resolution CD/ANPD No. 1/2021, another extremely important regulation that, added to the dosimetry criteria, ensures to processing agents the respect to the constitutional principles of due process of law, adversary proceedings, and full defense.

In an attempt to illustrate the impacts of the consolidation of privacy and data protection laws around the world as well as the conduct of national data protection authorities, we developed a survey that sought to identify, at a global level, the most prominent convictions in recent years, the evolution of the amounts of fines imposed and the scope of the penalized conducts.

Below, we present some reflections made based on the findings of this research:

Highest fines that reached the media



United States



China

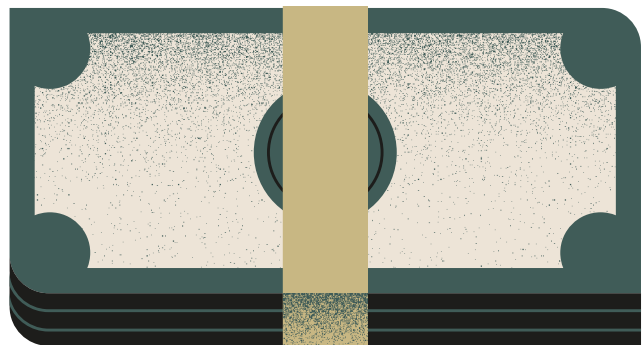


European Union



concentrate the highest fines, with sums ranging from hundreds of millions to billions of dollars. With iconic decisions, if there was any doubt, it has been demonstrated that there must be a new way of operating with data in the market: the convictions are aimed at punishing not only serious security incidents, such as leakage of personal data, but also the lack of transparency and adequacy to the legal bases and purposes for a legal processing of personal data.

Here we highlight the convictions with the highest fines imposed so far:



COUNTRY	YEAR	SECTOR	FINE	VIOLATION
 United States	2019	 Technology	USD 5 billion	Lack of transparency about the processing of personal data
 China	2022	 Technology	USD 1,2 billion	Collection of information through screenshots of the photo album of users' mobile phones and collection of facial biometrics from passengers without providing information to the data subjects and obtaining consent for the processing of the data
 Luxembourg	2021	 Technology	EUR 746 million (~ USD 877 million)	Processing customer data for direct marketing purposes without properly collecting consent for such purpose
 Ireland	2022	 Technology	EUR 405 million (~ USD 429 million)	Excessive exposure of children and adolescents' personal data due to the platform's default configuration, which allowed indiscriminate viewing by third parties of data such as e-mail and telephone numbers
 Ireland	2023	 Technology	EUR 390 million (~ USD 413 million)	Lack of transparency about the processing of personal data
 United States	2022	 Communication	USD 350 million	Failure to adopt effective information security measures, resulting in the leak of data of more than 75 million consumers
 Ireland	2021	 Technology	EUR 225 million (~ USD 255 million)	Failure to comply with transparency principles
 United States	2020	 Retail	USD 200 million	Failure to adopt information security measures capable of protecting the integrity of the data processed, resulting in the undue exposure of the data of 40 million individuals
 United States	2022	 Fintech	USD 190 million	Failure to adopt effective information security measures, resulting in the leak of data of over 100 million people

The application of fines in such proportions, however, is the result of an evolutionary process, and the European General Data Protection Regulation (GDPR), a reference for the creation of the LGPD and other countries laws, was also a leading event for the defense of privacy and the protection of personal data throughout the European Union.

GDPR without borders

Going beyond borders, the research revealed a great repercussion of the GDPR throughout the world, being patent the reinforcement of the protective nature of state power and the emphasis on coercive and punitive force.

An expansion of the sphere of privacy and data protection rights beyond the European Union was observed, a cascading effect largely driven by the mechanisms provided by the GDPR for the transfer of personal data outside the European Economic Area.

The impacts have also broadened the types of penalized breaches, until then essentially focused on consumer protection in cases of data leaks or illegitimate use of data to marketing. Even in countries without specific legislation on the matter, since the GDPR came into force, there has been a process of empowerment of data subjects over their personal information and a growing state action to repress the indiscriminate use of this information.





USA

In the United States, the largest fines prior to GDPR fell exclusively on serious incidents of personal data breaches and still represented a tiny percentage of the turnover of the convicted companies:

[KNOW MORE](#)



BRAZIL

Before the GDPR came into force and the edition of the LGPD, convictions in Brazil related to privacy and data protection were based on constitutional principles and the Consumer Defense Code, and the cases that reached the courts on a more recurrent basis dealt almost exclusively with situations in which there was the unauthorized use of personal data for direct marketing purposes, which led to modest convictions for moral damages - with amounts that ranged from R\$ 5,000.00 to R\$ 10,000.00.

[KNOW MORE](#)



United States



MID-2017

A hacker attack that exposed the data of approximately 40 million credit and debit cards triggered several lawsuits against Target, a company in the retail sector, resulting in convictions totaling **USD 18.5 million**.



MAY 2018



One of the largest incidents of personal data breach went to trial - the exposure of information from approximately 3 billion Yahoo! user accounts, with the company being ordered to pay a fine of **USD 35 million**.

With GDPR coming into effect, the fines increased significantly, and began to punish even situations that did not involve data leakage or direct damage to data subjects, but also the mere violation of transparency and autonomy of the data subjects regarding the control over the processing of their personal data:

OCTOBER 2018

Uber had to pay a fine in the amount of **USD 148 million**, for the leakage of data of 57 million users in a cybersecurity incident that occurred in 2016.



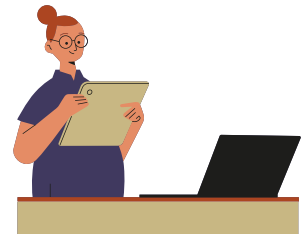
JULY 2019



Another trial led to the conviction of Equifax, also for data leaks. The initial fine of **USD 575 million** could reach **USD 700 million** by the end of the limitation period for data subjects harmed by the incident to file claims, which will only occur in January 2024.

MID-2019

The Federal Trade Commission ordered Facebook, Inc. to pay **USD 5 billion** for the lack of transparency and assertiveness in the information provided to users of its social network platform regarding the use and monetization of their personal data - the Cambridge Analytica case.



Brazil



Only in sparse, more iconic cases took place with fines of millions of reais, such as the conviction of one of the largest Brazilian telecommunication companies at the time at **1.5 million Brazilian reais** for unauthorized sharing of personal data, in 2017.

As of the second half of 2018, however, the repercussions of the GDPR were also felt in Brazil. In December, a drugstore chain was fined **R\$ 7 million** for the lack of transparency regarding the purposes of the processing of personal data on its platforms.

Facing major players in the market, in March 2021, Microsoft executed a Conduct Adjustment Agreement as a result of a Public Civil Action motivated by its collection of personal data without the due authorization of the users for the purposes of the processing, which involved the payment of **R\$ 2.5 million** for damages.

Continuing the trend toward higher fines, in June 2022, Decolar.com was required by Senacon to pay also **R\$ 2.5 million** for violation of the transparency principle regarding the use of data for geopricing practices.



Other Locations

Below is a brief comparison between amounts and motivations of convictions pre- and post-enforcement of the GDPR in different jurisdictions:



Hong Kong

HIGHEST CONVICTION BEFORE GDPR

HK\$ 16.000,00 (~ USD 2.040,00)



Lack of consent for use of personal data in direct marketing

HIGHEST CONVICTION AFTER GDPR

HK\$ 84.000,00 (~ USD 10.705,00)



Failure to respect data subjects' requests to cease processing personal data for direct marketing



Singapore

HIGHEST CONVICTION BEFORE GDPR

SG\$ 60.000,00 (~ USD 45.556,00)



Data leakage due to security breaches

HIGHEST CONVICTION AFTER GDPR

SG\$ 1 milhão (~ USD 759.270,00)



Data leakage due to security breaches



United Kingdom

HIGHEST CONVICTION BEFORE GDPR

£ 325.000,00 (~ USD 394.434,00)



Exposure of personal data due to security breach of deletion procedure

HIGHEST CONVICTION AFTER GDPR

£ 20 milhões (~ USD 24.272.900,00)



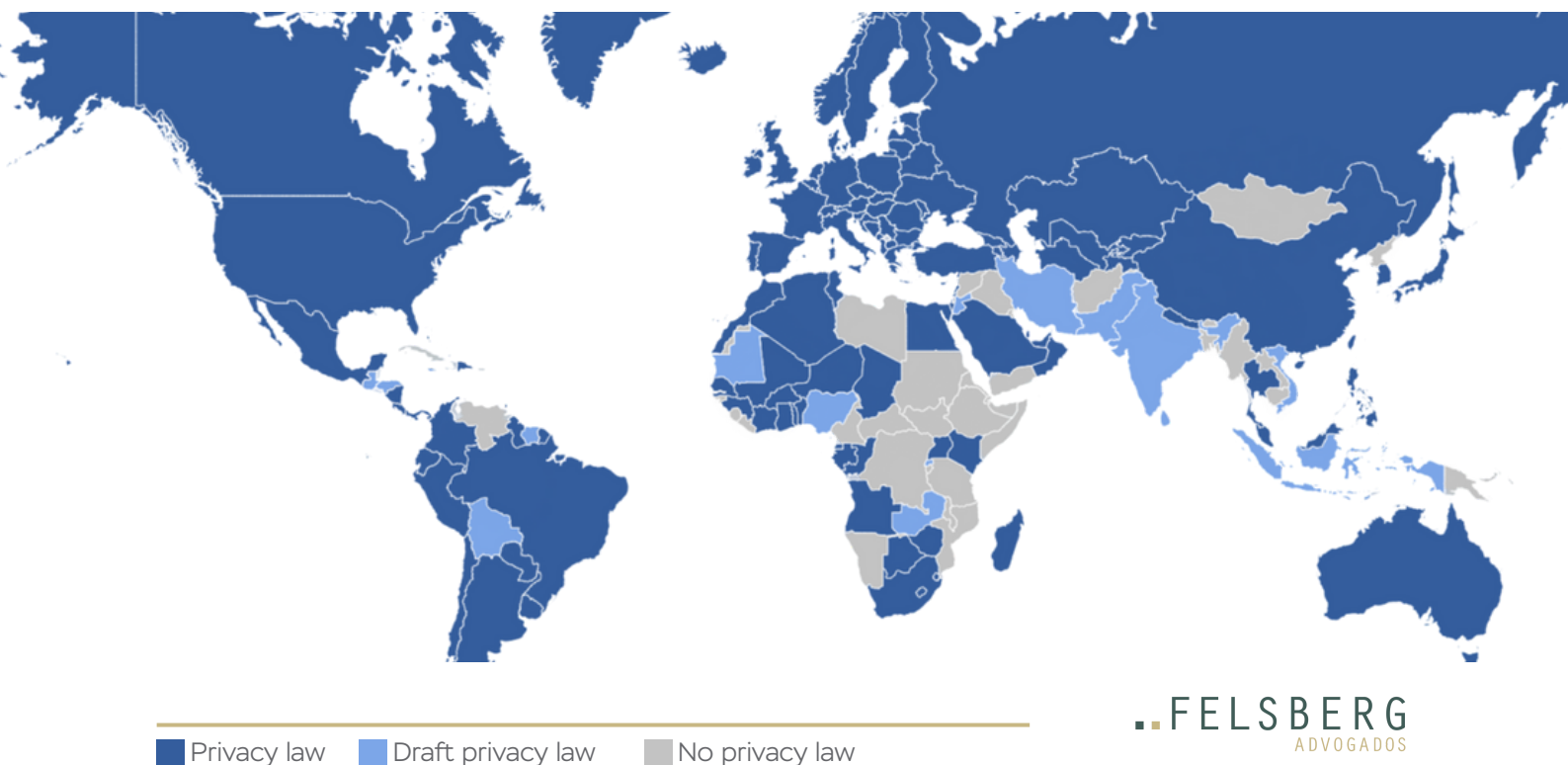
Data leakage due to security breaches

CONCLUSION

The analysis of the global panorama, from the historical perspective to the current moment, and the recent moves by the ANPD with regard to sanctioning measures reinforce the importance of the adequacy of the business activity to the LGPD. In the Data Era, taking the protection of individuals' information seriously is not just an option, but a crucial requirement for operating in the new market.

The consolidation of privacy and data protection rights at a global level require companies to be attentive to the principles that govern the regulation of these rights and seek to guarantee an ethical processing of personal data, otherwise companies will no longer be able to establish cross-border commercial relations.

The map below is a reflection of the global engagement in the issue and/or updating of standards protective of privacy rights and personal data protection:



National and international legislations have fostered an expansion of both the scope of protection and the amount of the penalties applied, being that the amount of the fines is only the tip of the iceberg of the setbacks caused to the company as a result of a conviction. Factors such as the loss of credibility and market value, the high investment necessary to re-establish the integrity of a system that has suffered a security incident and the subsequent monitoring of the affected data can represent inestimable financial and reputational impacts.

Privacy is here to stay. As informed by Waldemar Gonçalves in events celebrating Privacy Day, the complaints received by the ANPD so far exceed 6,900, a number that shows the evolution of a Brazilian privacy culture, in which individuals understand the value of their data and seek the guarantee of their rights.

The construction of an effective privacy and data protection governance program and the adoption of a respectful attitude towards data subjects have become basic requirements to gain the confidence of increasingly empowered consumers.

It is up to the companies to see the "glass half full" and transform the protection of personal data into a value aggregator to their products and services before the market and society.



2023

By: Daniela Machado e Míriam Ferreira
Layout: Anaís Moura
Coordination: Clarissa Luz
Privacy, Data Protection and Technology Team:
privacy@felsberg.com.br