

GDPR AND SANCTIONS: AN OVERVIEW ON THE EUROPEAN UNION

INTRODUCTION

Aware of the worldwide movement of enactment of privacy laws, application of sanctions, recognition of the protection of personal data as a fundamental right in the national territory and, mainly, considering the decades of experience in conducting judicial, administrative and arbitration proceedings in its area, the Technology, Media, and Telecommunications team of Azevedo Sette Advogados, through partners Ricardo Barretto Ferreira and Danielle Chipranski Cavalcante, and the Privacy and Data Protection Coordinator, Lorena Pretti Serraglio, prepared a special series on practical and technical issues involving personal data litigation.

The content begins with an overflight on the application of sanctions by foreign authorities – mainly, but not limited to, European authorities – and their eventual repercussions in the judicial scenario. And observing the international scenario is essential, since some trends can be reflected in Brazil, through the performance of the [National Data Protection Authority \(ANPD\)](#).

In relation to Brazil, subject matters will be discussed, such as the vacatio legis of sanctions and the illicit acts practiced in that period; the nature of civil liability; the consequences, for substantive law, of the recognition of data protection as a fundamental right; the applicable statutory period of limitation, especially considering the interdisciplinarity of the applicable laws; the practical aspects of reversing the burden of proof and the relationship with the Consumer Defense Code; proof of compliance with a decision arising from an obligation to do or not to do; the means of proof to demonstrate the deletion of personal data, in addition to many other points that will arise on the way. And you, reader, can be part of this project, sending suggestions of subject matters that you want to see discussed by our team.

Let's go together!

REGARDING THE EUROPEAN UNION, HOW HAS THE AUTHORITIES BEHAVED SO FAR?

In force for more than 3 years, the General Data Protection Regulation (GDPR) has substantiated more than 900 administrative sanctions and fines on the European continent. But it was more recently, especially in 2021, that the application of these penalties began to draw more attention, not only due to the increase in the number of impositions, but also due to the amount applied. In the third quarter of 2021 alone, the total penalties imposed represent almost € 1 billion, a number that is almost 20 times the sum of penalties imposed in previous quarters¹.

In a brief retrospective, we recall that in January 2020, the [Italian Data Protection Authority](#) imposed a fine of approximately € 27 million on a mobile operator. The infractions raised by the authority are diverse, but linked, in general, to the company's marketing activities, such as repeated promotional calls and sending unsolicited communications. Inappropriate handling of user consent records, excessive data retention and data exposure were also raised.

A relevant case involving the labor sphere (demonstrating the interdisciplinarity of the matters) took place in October 2020, when the [German Data Protection Authority](#) imposed a fine of approximately € 35 million on an apparel retailer. The grounds, in this case, were the

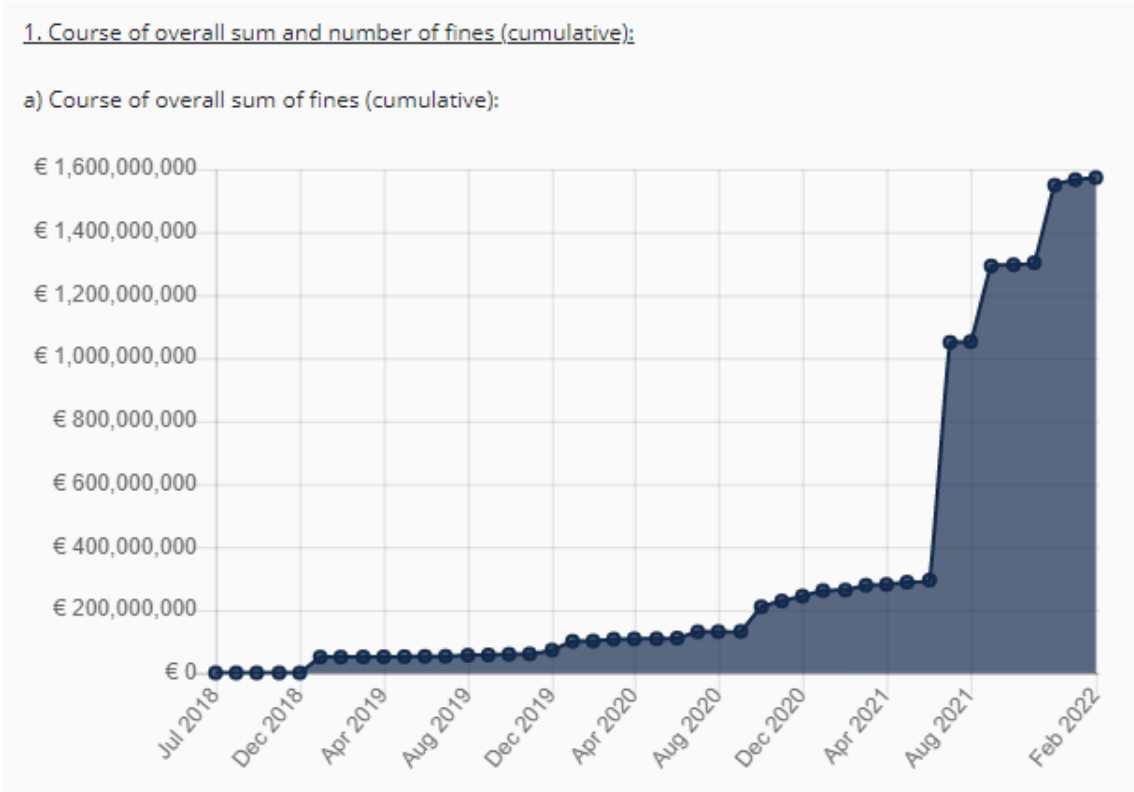
alleged monitoring of the network's own employees. After returning from vacation, employees had to attend a return-to-work meeting, which, at times, would have its content recorded and made available to various network's managers. The problem would lie at this point: whether the principle of data minimization would have been violated, according to which the collection and use of personal data, especially sensitive ones, should be limited to the directly relevant and necessary use, available only to those who are essential.

Regarding consumers' data, we recall that an airline was fined approximately € 20 million by the [UK Data Protection Authority](#), the Information Commissioner's Office (ICO), for a data exposure occurred in 2018. At the time, due to an alleged security breach, the company had its customers' personal data exposed, when, in the authority's view, this could have been avoided through the adoption of security mechanisms. It is worth noting that, in 2019, the ICO even pointed to an intended penalty of more than € 200 million. On similar grounds, the ICO imposed a fine of approximately € 20 million on a hotel company. The company would have been the target of cyber-attack, which culminated in the exposure of customers' data. Initially, the ICO had pointed to penalty amounts at the level of € 100 million.

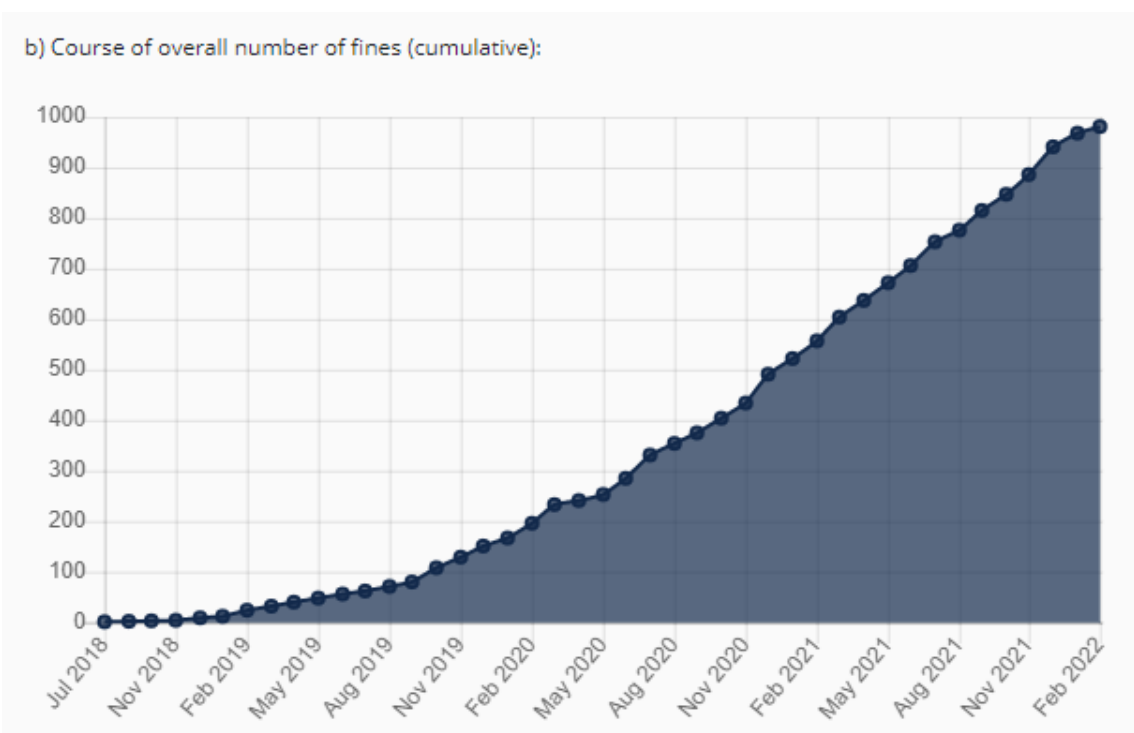
¹ The GDPR, it is worth remembering, authorizes the imposition of fines of up to € 20 billion or 4% of the company's global annual revenue, whichever is greater.

DATA PROTECTION LITIGATION

In 2021, we saw the increasing application of sanctions to technology companies. According to a graphic extracted from the website enforcementtracker.com, the total sum exceeded € 1.5 billion:



In February of this year, and until the date of this publication, there were already 981 sanctions applied:



Among them, there are sanctions applied by the [Irish Data Privacy Commission](#), imposing a fine of approximately € 225 million on a technology company for alleged lack of adequate explanation to users regarding personal data processing practices; by the [French Data Protection Authority](#), with the imposition of a penalty set at approximately € 90 million, in a claim related to the use of cookies.

Notwithstanding the numbers reproduced above, it is important to note that the imposition of penalties does not necessarily mean that it is not possible to adopt actions or appeals that may result in the legitimate removal or substantial reduction of amounts. The interpretative variable of the sanction applicator cannot be left out – considering the biggest ones known, there are penalties imposed by Luxembourg, Ireland, Italy, France, Germany, United Kingdom, Spain, Sweden, and the Netherlands, for example.

Some of these interpretations are being considered extremely rigid, culminating in fines classified by the market as ambiguous or inconsistent, instigating legal battles in the coming years. And this is the scenario that is envisaged for the near future in Brazil, especially in view of the existence of other bodies also active in this scenario, especially those for the protection of consumers' rights, such as Procon and Senacon. These, we know, have already applied fines based on the LGPD, as we will see later in this series.

Thus, even in the midst of uncertainties, the practical view of the application of the GDPR is extremely relevant and can guide the steps of the ANPD; not only in terms of quantitative setting of penalties, the problems experienced also serve as a guide for issues that will potentially be experienced in Brazil, and that will inevitably end up in the national Judiciary.

AUTHORS



Ricardo Barretto Ferreira da Silva
barretto@azevedosette.com.br



Danielle Cavalcante
dcavalcante@azevedosette.com.br



Lorena Pretti Serraglio
lserraglio@azevedosette.com.br



Carolina Simioni Perdomo
cperdomo@azevedosette.com.br