



TMT Retrospective | 2018

Azevedo Sette ⁵Years
ADVOGADOS

..... We are +50

RECONIZED AS ONE OF BRAZILIAN LAW FIRM WITH THE HIGHEST VOLUME OF M&A DEALS SINCE 2015.

M&A Rankings - Bloomberg, Thomson Reuters and Mergermarket

“THEY ARE KNOWLEDGEABLE, UNDERSTAND OUR BUSINESS WELL AND HAVE MANY YEARS OF EXPERIENCE IN THE FIELD”

Chambers Latin America

“A CLIENT COMMENTS DESCRIBES THEM AS THOUGHTFUL, WELL-PREPARED LAWYERS WITH HIGH-QUALITY STANDARDS, ADDING THAT, MOST OF ALL, [THEY ARE] ALWAYS AVAIABLE.”

Latin Lawyer 250

“THE FIRM ACTS FOR AN IMPRESSIVE PORTFOLIO OF BRAZILIAN MULTINATIONAL CLIENTS AND OTHER REPRESENTATIVE NAMES.”

The Legal 500



Azevedo Sette São Paulo Office

Introduction

With wide expertise in the high-tech segment and alert at all times to the ongoing process of technological evolution, expansion of the technology market, and the complexity of regulatory frameworks governing the sector, Azevedo Sette Advogados has worked to assemble and consolidate a specialized team to serve the growing demand of clients in the IT, Media, Internet and Telecom sectors.

The team is formed of distinguished, multilingual and experienced lawyers with long-standing experience of the telecoms and technology sector, admired for their proven track record in the full range of IT matters, including hardware supply and software distribution, development and implementation. Further capabilities cover e-commerce matters and multimedia payment platforms. Team is also well versed in assisting with telecoms deals, regulation and infrastructure mandates.

The group works cooperatively with regulatory, antitrust, corporate, tax, and litigation lawyers in dealing with such matters.



Azevedo Sette São Paulo Office

Authors

Ricardo Barretto Ferreira da Silva, *partner and head of TMT*

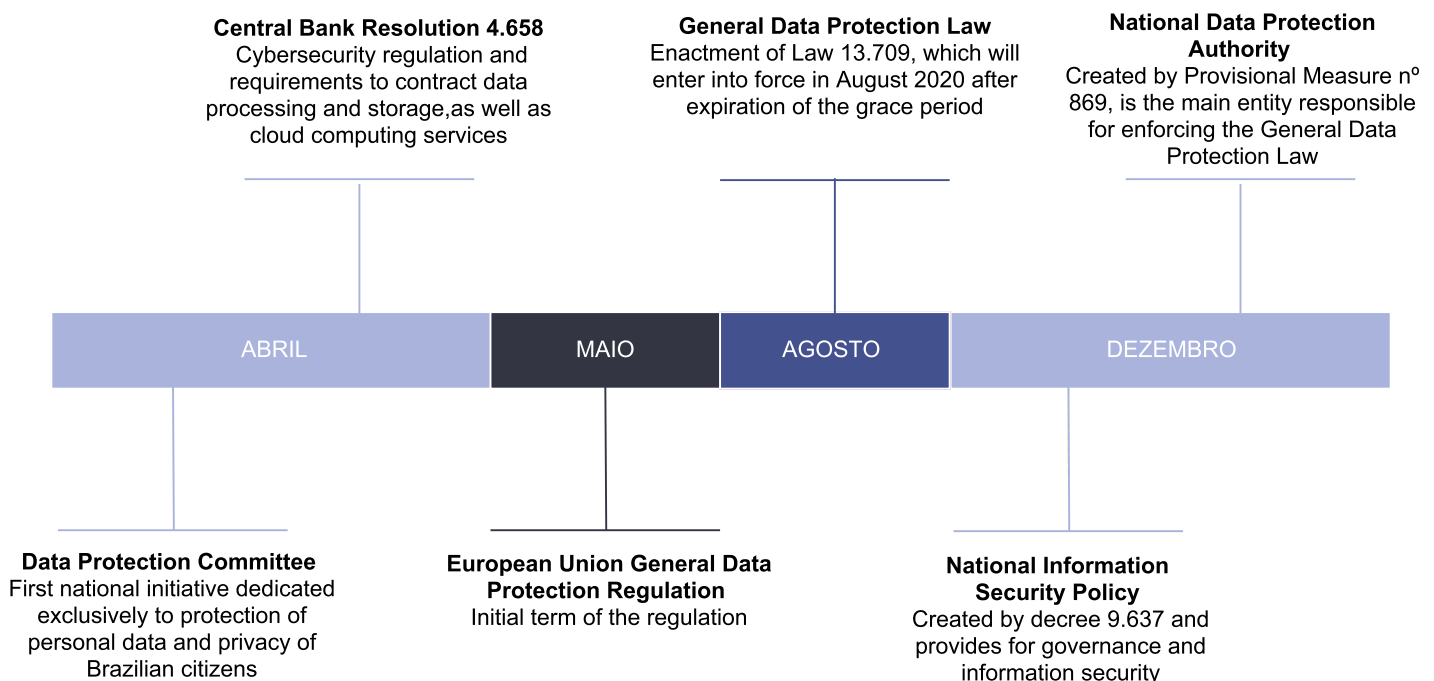
Lorena Pretti Serraglio, *lawyer*

Vitor Rodolfo Koketu da Cunha, *trainee*

2018 and the focus on privacy and data protection

The year of 2018 was outstanding for the regulatory framework governing privacy and data protection, in Brazil and in the world. The subject gained great significance due to the modernization of technologies, emergence of applications and changes in social behavior. Information became society's new defining element, as machines and electricity once were.

Within this context, in a movement towards adequacy to social facts, in May 2018 the General Data Protection Regulation or GDPR came into force. Locally, we are facing Resolution 4.658, issued by Central Bank, approval of the General Data Protection Regulation in Brazil and Provisional Measure nº 869, which created the National Data Protection Authority (ANPD):



National authorities, regulations and laws

The Personal Data Protection Committee is an initiative of the Public Attorneys' Office of the Federal District and Territories. Based on constitutional roles of the Parquet itself, it has been acting in several incidents with grounds on seven pillars:

- **Opinions Pillar**, which proposes directives for a National Policy on the subject matter;
- **Information Pillar**, to inform the population, companies and public entities about public rules and policies on data protection and privacy;
- **Studies Pillar**, to promote national and international studies, in particular in view of the lack of borders pertaining to use of data;
- **Cooperation Pillar**, to cooperate with data protection authorities, including on an international level;
- **Notification Pillar**, to receive communications about security incidents that may cause damage to data subjects;
- **Investigation Pillar**, to file preliminary proceedings, civil public inquiries and administrative proceedings, also jointly with the natural prosecutor.
- **Sanction Pillar**, to file the competent legal actions, jointly with the case's natural prosecutor.

Also, with regard to consumer protection, we point out to the **National Consumer Secretariat (SENACON)**, an entity subject to the Ministry of Justice, with responsibilities prescribed by the Consumer Protection Code (CDC), which had active roles in some cases involving privacy and data protection in 2018.

Moreover, specific rules were created to certain areas of the economy. By way of example, Central Bank of Brazil published Resolution n° **4.658/2018**, which provides for cyber security policy and requirements to contract data processing and storage services, as well as cloud

computing, to be complied with by financial institutions authorized to operate in this field.

The purpose of these regulations, including the one issued by the Central Bank of Brazil, is to control how organizations, companies and the government itself use massive quantities of personal data produced by them, with a view towards protecting users/individuals from unauthorized, improper and malicious use. Without effective rules and without supervision by the competent authorities, collected data may be used improperly, exposing users, in their capacity as consumers, to risks and occasional losses.

The **General Data Protection Law**, enacted in August 2018, will be an essential prop to support actions undertaken by the competent authorities. Expected to enter into force only in August 2020, it grants a grace period for companies to conform to the new data protection regulation. Those who think that this is a long period are mistaken. The way companies operate will be directly affected and for this reason a deeper look at the dynamics of data will be crucial, which ultimately will result in adjustments.

Therefore, from a statutory and regulatory point of view we notice that Brazil is taking a discerning look at information virtualization in order to adjust its legal framework to current social facts, thus ensuring that citizens will have proper assistance and support, when required.

MPDFT systemic operation

As seen, 2018 was marked by the continuous operation of the Public Attorneys' Office of the Federal District and Territories (MPDFT), that created the Personal Data Protection Committee, current Artificial Intelligence and Data Protection Unit – ESPEC, the first national initiative solely dedicated to the protection of personal data and privacy of Brazilian nationals. The committee acted systematically on several cases involving breach and improper use of personal data.

One of the first cases involves breach of data held by Netshoes, an e-commerce company. At that point in time, 2 million customers were affected by the breach of data including names, tax ID number, CPF, e-mail, date of birth, purchase code and purchase price. Such breach made public data that not only distinguished each user but also their individual profile as consumer.

Despite the fact that currently there is no legal provision establishing the obligation to inform data breaches to affected users and to the general public (in particular due to the grace period determined by the LGPD), the Public Attorneys' Office, with grounds on legal principles and taking into account the severity of the incident and risks deriving from the exposure of personal data advised, through the Personal Data Protection Committee, that the e-commerce company Netshoes should:

- Notify customers affected by the security incident by means of a letter, with return receipt (AR) or a telephone call, informing which personal data is involved in the incident (failure to do so would result in a public civil action for moral and material damages caused to consumers¹);
- Refrain from making any kind of payment to the alleged perpetrator of the security incident, subject to characterizing procedural fraud².

The Committee also investigated the breach of data held by Uber, which affected 57 million accounts of company's drivers and customers around the world, including data of 156 thousand Brazilian users, such as name, telephone number

submitted to the General Manager of Uber in Brazil, inquired the company about the data pertaining to Brazilian drivers and customers affected by the incident. After the Committee's inquiry, Uber decided to notify the affected customers and to inform them about the incident.

With regard to the breach of data held by Banco Inter, the Committee filed a Public Civil Action (ACP) against the financial institution requesting the court to order the bank to pay a compensation for moral damages in the amount of R\$ 10 million for failure to take the necessary precautions to ensure the security of personal data of customers and non-customers of the institution.

According to the ACP, Banco Inter informed a security incident in which personal data of customers and vendors were breached. The Committee received from Central Bank of Brazil the customers' data that was breached, including bank, tax ID, account number and full name of the titleholder of the account, individual or legal entity. Approximately 13.000 accounts/customers had their banking information compromised and the data was being sold in the Deep Web.

On December 18, 2018, the court approved a settlement between the MPDFT and Banco Inter. The settlement establishes payment of R\$ 1 million to government entities that fight cyber crimes and of R\$ 500 thousand to charities.

In addition to the cases mentioned above, the Committee is also investigating the following security incidents and improper use of personal data:

¹

http://www.mpdft.mp.br/portal/pdf/comissao_protecao_dados_pess_oais/Recomendacao_Comissao_Protecao_Dados_2018_01.pdf













²

Same

MPDFT systemic operation

MISUSE OF PERSONAL DATA

SECURITY INCIDENTS

		NETSHOES	Public Civil Inquiry Recommendation to notify 2 million users about data breaches in Brazil
		UBER	Preliminary Proceeding Settlement to notify 196 thousand Brazilian affected by the incident in Brazil
Public Civil Inquiry Investigation about the circumstances and possible causes of probable unlawful use of personal data of Brazilian citizens	 Cambridge Analytica	 twitter	Request for information Information requested in view of 300 millions users affected by the incidente in the world
Public Civil Inquiry Investigation about how YouTube treats data of Brazilian children	 YouTube	 inter	Public Civil Action Settlement of 1.5 million in consideration for collective moral damages resulting from data breach of 13 thousand customers
Public Civil Inquiry Investigation about use of facial recognition technology of Facebook users and non-users	 facebook	 C&A	Preliminary Proceeding Monitoring the consequences of an incident involving 2 million users affected in Brazil
Public Civil Inquiry Investigation about use of biometric databases and facial recognition algorithms for commercial purposes	CredDefense Certibio Acesso Digital	 MyHeritage DNA	Request for information Information requested due to breach of data pertaining to 3.5 million users affected in Brazil
Public Civil Inquiry Investigation on the legality of smartphones' tracking tool in Brazil	 inlocomedia	 SKY	Public Civil Inquiry Investigation about a possible security incident involving data of 32 million customers
Public Civil Action Unlawful commercialization of personal data of Brazilian citizens over the Internet	Text  tudosobre todos	 FIESP	Public Civil Inquiry Investigation about a possible security incident involving data of 34 million Brazilian citizens
		 g+	Public Civil Inquiry Investigation about personal data of Brazilian users affected by a security incident involving 52 million users around the world

SENACON and PROCON/MG actions

Apart from the cases described above, other consumer protection entities also had active roles in cases involving breach and/or improper use or disclosure of personal data.

The National Consumer Secretariat (SENACON) imposed a fine to the site Decolar.com in the amount of R\$ 7,5 million for offering different prices to hotel reservations depending on where the consumer was located (practice known as geo pricing) and for hiding the availability of accommodations to Brazilian consumers to benefit foreign consumers (practice known as geo blocking). SENACON considered such practices abusive and discriminatory, in clear violation of consumer laws that state that suppliers of goods or services are not allowed to:

- Deny requests from consumers to the exact extent of their stock availability;
- Deny sale of goods or services to whom is willing to purchase them on a cash basis;
- Increase the price of goods or services without just cause.

In addition to the above mentioned fine, the company was ordered to immediately cease abusive and discriminatory practices, subject to having its operations suspended and the site shut down.

In another case involving misuse of personal data, the network of drugstores Drogoria Araújo received a fine in the amount of R\$7 million imposed by Procon-MG for making discounts available to consumer only in case they informed their tax ID (CPF) at the time of the purchase, without giving any clear and appropriate information about their registration.

The order resulted from an inquiry involving the facts and the company's refusal to adjust its conduct. According to the decision, this practice violates consumer's right to clear and appropriate information about the service being offered, since the drugstore failed to properly inform consumers about its terms of use, privacy policy and risks to the program's data security.

Data relative to purchases at a drugstore may reveal sensitive information about consumers' health and life that may lead to abusive practices by companies. Diseases, mental problems and other sensitive information may be deduced based on purchase habits at drugstores and this information is not clearly provided to consumers. Therefore, a consumer, the party in disadvantage in this relationship, did not have the information required to properly consent to the collection of personal information in exchange for the discount.

According to the public prosecutor at the consumer protection court of the district of Belo Horizonte, Fernando Ferreira Abreu, "the main scope of the alleged rewards program is to collect consumers' tax ID and not to establish a rewards or loyalty program, per se", and this constitutes an abusive practice because discounts cannot be conditioned to the provision of personal information.

Pursuant to the decision, "constant collection of information concerning consumers purchase habits, performed in a concealed way and without prior information, poses great risk to consumers' intimacy and private life, as well as subjects them to other risks of different kinds".

The cases above are proof that the grace period of the LGPD has not been an impediment to investigations and to have companies held accountable for their actions, so much so that the operations that took place in 2018 represent a small sample of what is to come, in particular vis-à-vis the effectiveness of data protection regulations, in Brazil and abroad.

What to expect for 2019?

In accordance with a study³ performed by Gartner consultants, expenses with products and services associated with information security will reach \$124 billion in 2019, a growth of 8.7% in comparison with 2018. This estimate reflects the challenges, without precedent, involving cyber security and data protection faced by companies (of all sizes, it is important to mention).

Digital threats develop at the same pace as technology progresses. We are not talking about a distant reality here, but rather about what is happening around us on a daily basis: technologies that are becoming more and more usual in a digital society, including facial recognition, the Internet of things, Internet 5G, drones, big data, artificial intelligence, DNA mapping, self-driving vehicles, smartphones, smart watches.

All technologies above are changing the limits and expectations of privacy, posing new challenges to civil society, the government, regulatory agencies, companies and organizations. If 2018 brought to light so many incidents, it made the reality of facts quite clear, that is, action and caution must be exercised to protect our data, no matter if we are in the capacity of data subjects, operators or controllers.

Information security is a key factor to transform the digital society. And, in view of what had been studied so far, some behaviors may be crucial in corporate environments to prevent problems in the future, such as compliance with data protection regulations, local and international, risk analysis involving digital businesses and protection of intellectual property in online environments. To adopt a conduct compliant with applicable laws and regulations is the first step towards mitigation of so many risks.

And what about the year that is just beginning, what can we expect? Well, the first weeks of 2019 already combined two huge events. On January 17, a digital security researcher found a database with approximately 773 million unique e-mails and 21 million unique passwords⁴, in one of the largest data breaches of the history. On January 21, the French data protection authority, CNIL, ordered

Google to pay a 50 million Euro fine for lack of transparency and informed consent regarding its advertisements, as well as improper information.

Hence, it is clear that companies dealing with data are subject to security incidents. And, here, we include them all: giant technology companies and small neighborhood ventures. The cost associated with these incidents is high: identification of the problem, notice to users, regulatory fines, loss of reputation and business.

These considerations lead us to conclude that a preventive conduct is the best strategy. Get to know your business, what sort of data is collected and how it is treated. Look carefully to the tools you use and, if necessary, seek an expert.

3

Available in English at <https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019>

4

Available in English at <https://www.troyhunt.com/the-773-million-record-collection-1-data-reach/>



BELO HORIZONTE (MG)

Rua Paraíba, 1000 | Térreo
30130-141 | Tel.: +55 11 3261.6656

BRASÍLIA (DF)

Setor Hoteleiro Sul, Quadra 6, Conj. A, Bl. C | 20º andar
70316-109 | Tel.: +55 61 3035.1616

GOIÂNIA (GO)

Rua 10, 250 | Conj. 507, Edifício Trade Center, Setor Oeste
74120-020 | Tel.: +55 62 3096.4573

RECIFE (PE)

Av. Gov. Agamenon Magalhães, 4575 | 4º andar
50070-160 | Tel.: +55 81 3019.0020

RIO DE JANEIRO (RJ)

Rua Sete de Setembro, 99 | 17º andar,
20050-005 | Tel.: +55 21 3550.5900

SÃO PAULO (SP)

Av. Pres. Juscelino Kubitschek, 2041 | Torre E | 16º andar
04543-011 | Tel.: +55 11 4083.7600



  www.azevedosette.com.br

