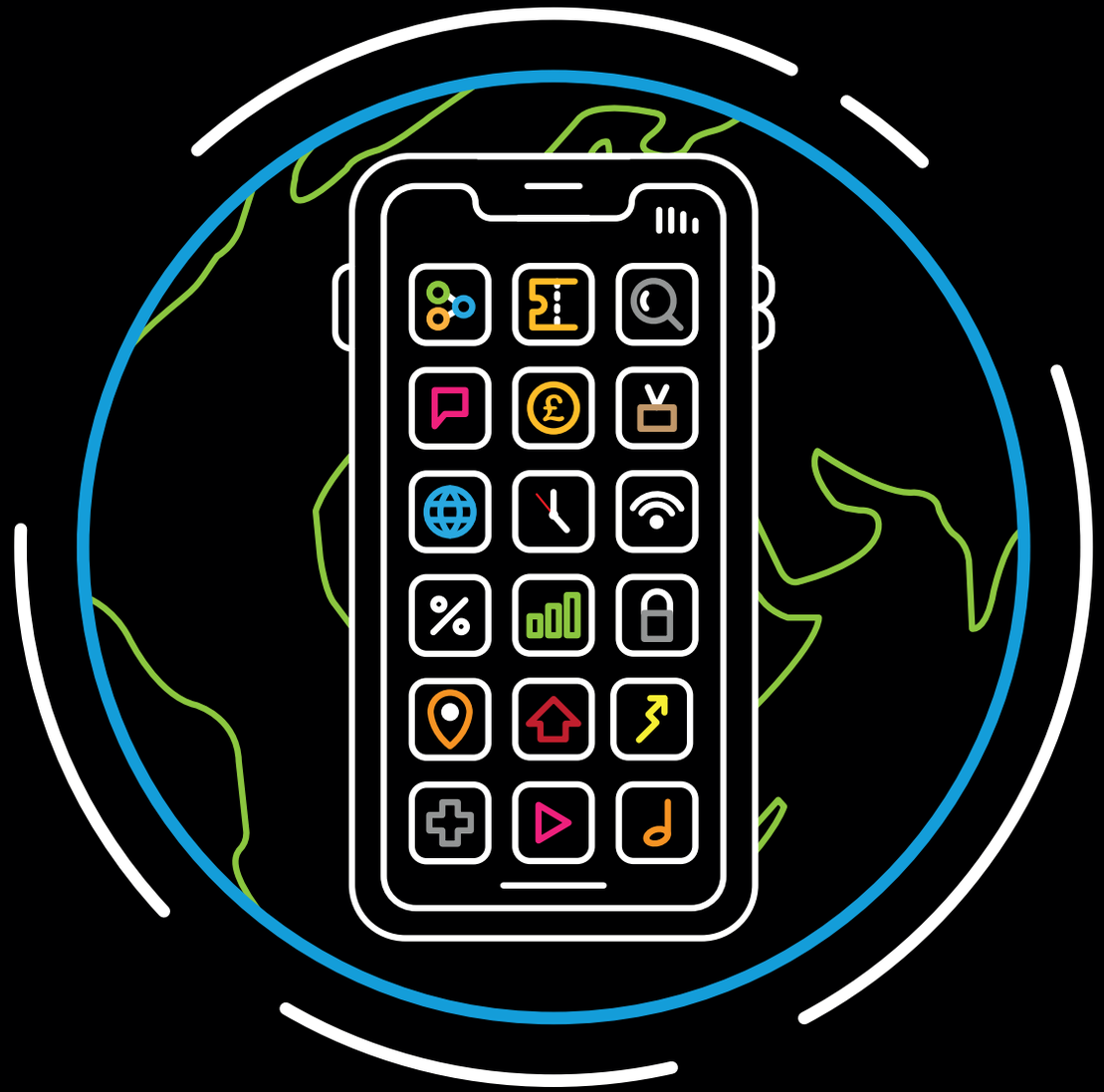
INTERNATIONAL ASSOCIATION OF ENTERTAINMENT LAWYERS

# Nationalism vs globalism: regional and transnational legal issues reshaping the entertainment industry

Edited by William Genereux & Marijn Kingma



# IAEL 2020

## "Nationalism vs globalism: regional and transnational legal issues reshaping the entertainment industry"

**Editors**
William Genereux
Marijn Kingma

**Publisher**
FRUKT
www.wearefrukt.com

**Design**
Lauren Cotterell
Rashpal Amrit



# Message from the President: Jeff Liebenson

I hoped this year of 2020 would be marked by our pursuit of this very interesting and relevant topic of Nationalism vs Globalism. And also my tenth year of serving as President of the IAEL, which is and continues to be such an honor.

But we are confronted by a pandemic that has affected our world. As we go inward to avoid mass contagion and yet continue to hear about its devastating effects across the globe, it sometimes is difficult to think of anything else. I echo the co-editors' hope that normalcy will to some degree return soon.

I am quite certain that the subject chosen by our co-editors will remain relevant. So in that spirit, we move on.

At times like this, it's inspiring to see the IAEL do what the IAEL does best—focusing on the key issues of the day, and enjoying the collegiality of our fellow members across national boundaries.

So while the world is going through distancing and isolation, the IAEL has come together to mount its first-ever digital IAEL Legal Summit. This has been a true group effort with major contributions from different corners of the world, bringing our different backgrounds and perspectives to work together across national borders.

I want to thank Marijn Kingma from The Netherlands and William Genereux from Canada, our co-editors who have brought their experiences from where they live and their legal expertise to life in developing this book, as well as our contributors for providing their rich perspectives.

Thanks to Duncan Calow and Marcel Bunders for your continued support, guidance and humor with respect to the many adversities we have weathered this year!

While the book focuses on digital and other entertainment deals crossing borders, it also addresses what legal needs still should be considered on a national or country-by-country basis. Our hope is that exploring these legal trends will help us in guiding our clients to deal with our multicultural world of entertainment law, notwithstanding the nationalistic urges of our time.

Perhaps this mirrors our staging of this digital IAEL Legal Summit with members from around the world enjoying our different cultures and coordinating our common interests.

We look forward to the upcoming publication of this, our 35th annual book published by the IAEL, Nationalism vs Globalism: Regional and Transnational Legal Issues Reshaping the Entertainment Industry.

# Editors' Introduction:
## William Genereux & Marijn Kingma

When this year's topic 'nationalism vs globalism' was chosen at the IAEL general meeting in 2019, no one could have foreseen that our world would soon be faced with a global pandemic. As we are writing this, COVID-19 has halted normal life throughout the world. With countries taking extreme lockdown measures, the impact on the economy is unimaginable and the entertainment industry had been brought to a near standstill. Concerts, festivals, movie releases and other events have been cancelled and entertainment lawyers are faced with unprecedented legal issues. But the entertainment industry is also proving its creativity in these times with initiatives like drive-in festivals, balcony concerts and virtual movie watching parties.

It was unavoidable that Midem, where we present our annual IAEL book each year, was cancelled. This has led to the decision to hold our 2020 IAEL book so that we can present it to the IAEL community at next year's Midem. The book will be released as the "IAEL 2020-2021" book. We believe the topic and content of the book will remain relevant.

However, we did not want to refrain from publishing anything at all this year, so we have decided to release five contributions from our book for next year as a 'sneak preview.' We believe the chapters we have chosen are a good reflection of our book and are also great standalone reads.

Our 2020-2021 book will explore the longstanding conflict between nationalism and globalism as it relates to the entertainment industry. Contributions will be subdivided into three major categories. The first category focuses on issues in specific jurisdictions and markets. The second attempts to map-out the expansion of regional forces into wider applications. The third seeks to bring a holistic view that reconciles many of the vital issues affecting the industry at large, and which are shaping our future world.

As a sneak preview from the first chapter, we have chosen a contribution about the effects of Brexit on the entertainment industry, a topic that cannot be missed in a chapter about regionalism. From the second part of our book, we have selected two articles about the effect of the GDPR around the world, as countries are adapting their data protection legislation to keep up with Europe's strict rules. Finally, we have released two contributions from the third chapter of the book. The first looks at the (im)possibility to regulate fake news and political advertising on social media platforms. The second article is about what is no doubt the biggest challenge of our times: global warming. The article discusses environmental impacts of recorded music and what we as lawyers can do to help mitigate climate change.

The fast spread of the virus is a direct result of globalization – international air traffic has quickly moved it around the world. And while countries are all imposing their own countermeasures, the virus knows no national borders. Meanwhile, globalization may also halt the virus. The global scientific community was able to find a reliable test for COVID-19 within days and is now working together to find a treatment and a vaccine. We are hoping that by the time our book comes out in 2021, global efforts will have resulted in a return back to – relative – normalcy.

We would like to thank IAEL's president Jeff Liebenson for his time, effort and leadership. We would also like to thank Janneke Popma, associate at Höcker, for her indispensable organizational skills. Additionally, the authors all need to be recognized for their creativity and their understanding when we had to postpone the release of the book.

Thank you everyone.

### >> William Genereux

TORONTO

William is a Toronto lawyer with 35 years' experience in entertainment law, corporate law and litigation. In the 1980s he played in a hardcore punk band. In the 1990s he co-owned and operated a dance music record label. In the 2000s he was a lecturer at the Ted Rogers School of Management – Ryerson University, Toronto. His clients include top-selling recording artists, producers, writers, digital technology entrepreneurs and filmmakers. He is a member of the Law Society of Ontario, volunteers with Artists' Legal Aid Services in conjunction with the University of Toronto Faculty of Law, and is a past-chair of the Canadian Bar Association – Ontario, Entertainment, Media and Communications Law Section.

### >> Marijn Kingma

U.S.A.

Marijn Kingma is a partner at Höcker Advocaten, based in Amsterdam. Marijn specializes in information law, with a focus on copyright and privacy-related issues. Marijn has a varied practice; her clients range from collective management organisations and NGO's to broadcasters and international entertainment companies. She conducts complex, strategic litigation and has been involved in several national and European landmark cases. Marijn is ranked in the Chambers guide as a "very strong, young up-and-coming lawyer" who is "unbelievably good and very clever" and is ranked in the Legal500 guide as "next generation lawyer", noting that "her knowledge, flexibility and positive mood makes working with her a fun, but still very effective experience". She is editor for the Dutch law journal AMI, an active member of the International Association of Entertainment Lawyers and a regular speaker at (national and international) conferences.

# The Brazilian General Data Protection Law and the rise of a new era of privacy standards in Latin America

"Personal information is a highly regarded right, subject to indemnification in the event of infringement that results in material or moral damages."

**Authors: Marcelo Goyanes and Leticia Carneiro**

*Marcelo Goyanes: Marcelo is a founding partner of Murta Goyanes Advogados, and advises on media, entertainment, and intellectual property law. He is ranked in the last editions of Chambers Global and Who´s Who Legal. In 2019, Marcelo was granted the award "Client Choice, by Lexology" for Brazilian Copyright Lawyer of the year. For over 20 years, Marcelo has represented local and international clients including film producers, TV channels, platforms, and aggregators, advertising and media organizations, record companies, and talents in various markets, such as audiovisual, music, literature, games and art. Marcelo has a master's degree from the George Washington University. His strong academic profile has seen him lecture at well-known Brazilian academic institutions and universities since 1999. He has also authored a book, many law review articles (published both in Brazil and abroad), and was co-editor for two books published by the International Association of Entertainment Lawyers (IAEL): The Monetization of the Global Music Business and The Streaming Revolution in the Entertainment Industry. He was appointed general counsel of the Brazilian Association of Industrial Property Agents, and he is a member of the IAEL's executive committee.*

*Leticia Carneiro: Leticia is an associate at Murta Goyanes Advogados, and has experience with law firms and local authorities, specializing in intellectual property since 2017. With knowledge in law and technology, she was indicated to Miranda Rosa award for her Bachelor of Laws final course assignment about algorithms and social media providers. Leticia assists domestic and foreign clients, with emphasis on litigation, advising on data privacy and internet issues, as well as dispute resolution, unfair competition and border measures.*

## 1. Introduction

On August 2018, Law No. 13,709/2018 (the Brazilian General Data Protection Law - "LGPD") was enacted, aiming to regulate the use and protection of personal data in Brazil. According to the text approved on July 2019, the LGPD should enter into force in August 2020, after several modifications performed by the National Congress and the former and current Presidents between 2018 and 2019, as well as eight years of discussions of the Bill of Law in the Brazilian Legislative branch.[1]

From the modifications applied, the Brazilian law represents a clear attempt to align local norms with international legislation and more specifically to the European Union ("EU")´s General Data Protection Regulation ("GDPR"), and therefore enable the transfer of personal data to Brazil, after the GDPR has limited the transfer of personal information to countries that guarantee the same level of protection as the EU legislation.

Differently from European Union nations, Brazil has not experienced legislations focused on personal data protection so far. Despite Law 12,965/2014 (the Brazilian Civil Rights Framework for the Internet - "Marco Civil"), which broadly addresses the use of Internet in the country, and briefly approaches personal data issues, it is possible to state that Brazilians courts, companies, public institutions and citizens have not faced strict legal obligations regarding data protection until the LGPD.

This article aims at analyzing the LGPD and its possible impacts on the Brazilian society, considering the lack of history with data protection in Brazil. In addition, it will address how this legislation echoes EU's GDPR, since the Brazilian language is similar in many aspects to the concepts and principles adopted by the European legislation.

### 1.1.The Brazilian legislation on personal data protection before LGPD

The legal protection for personal data is considered part of the right of privacy, foreseen in 1988's Federal Constitution ("CRFB/88") as a fundamental right[2]. According to CRFB/88, privacy - and therefore personal information - is a highly regarded right, subject to indemnification in the event of infringement that results in material or moral damages[3]. Despite the understanding that personal data is protected by the Constitution since 1988, it clearly required a specific regulation in order to fully secure the respect to citizens' information, as well as address the complexity of the matter. In

"Even though personal data protection is often cited in accordance with the Marco Civil, it is also closely related to the rights to privacy and intimacy."

importance and protection of personal data, being used as grounds in the enforcement of data protection cases involving service providers in general, including situations around access and Internet application providers[4]. Considering the resemblance of the relation between these two kinds of providers and their users to a consumerist relation[5], the CDC is often used as a basis for the application of penalties in the event of infringements, subordinating access and Internet application providers to this Code's dispositions - despite the differences between the nature of the services offered by "technology" providers and others.

As an example, section VI of the CDC specifically states that consumers shall have access to their personal data stored by providers. This information must be objective, clear, truthful and of easy comprehension, and it is forbidden to store data regarding consumers' financial debts for a period longer than five years.

The Consumer Protection Code also provides for a right to request the correction of stored personal information with inaccuracies and presents a more direct approach to personal data protection when compared to the Federal Constitution. Users are seen as consumers and the rules applied expressly focus on personal data protection, and not only privacy at large. The fact that a right to data protection was explicitly mentioned represented an important development in early 90´s. However, data protection was still limited to a consumerist context and the regulation lacked the details and depth needed for the complex subject of personal information in the information technology era.

With the Marco Civil of 2014, data protection was finally described as a principle and right separated from the protection of privacy[6]. This change was a demonstration of the need to have a proper law to regulate the use of personal information in Brazil.

Even if still associated to privacy matters, the protection of personal data afforded by the Marco Civil was granted in different articles, starting to outline rules that would be included in future Brazilian General Data Protection Law. As an example, Marco Civil requires the freely given , explicit and well informed consent of the data subject to allow the treatment and sharing of personal data with third parties, as well as demands the provision of clear and complete information regarding the collection, use, storage, treatment and protection of individual's personal data.

Moreover, Brazilian Civil Rights Framework for the Internet establishes penalties for the violation of an individual's personal data rights, which includes (a) warnings; (b) fines up to 10% of a Brazilian economic group's turnover in the last annual report; (c) temporary suspension of the activities involved in the infringement; and (d) the prohibition of such activities. As will be further discussed, the last two penalties were vetoed in the final text of LGPD, for being considered harmful to the functioning of important financial institutions in the country.

**1.2.The enforcement of personal data protection in Brazil before LGPD**

The enforcement of personal data protection has not reached the local courts in broad and relevant cases so far, despite several data breaches reported by the media[7]. Instead, the case law is limited to two situations: (a) credit scoring and other cases regarding consumerist's relations based on the application of the CDC; and (b) the right to be forgotten and the right to de-indexation, based on Marco Civil and the Federal Constitution.

Still, even though personal data protection is often cited in accordance with the Marco Civil, it is also closely related to the rights to privacy and intimacy, being used to justify the de-indexation of personal data in search results in cases involving the right to be forgotten. Considering the matters discussed in this type of cases, it creates the impression that personal data protection is an important individual right only if analyzed from the perspective of the right to be forgotten - meaning, the right to have personal data removed after a reasonable period of time and in cases in which there is no public interest in accessing one's personal information.

On the other hand, consumer protection cases present a more protective approach to personal data. Courts usually secure individual´s rights to access the information gathered by service providers, as well as impose fines to the non-authorized use of consumers' personal information by third parties - that are mostly characterized by Courts as data breaches. However, the application of the CDC is restrictive to its purposes, as it cannot be considered a specific legislation on personal data protection.

"In Brazil, the time between the occurrence of a data breach incident and its containment takes almost an entire year."

In this context, based on the CDC and the Federal Constitution, the usual indemnification granted by Courts to entities who violate personal data regulations in Brazil range between R$ 2,000 and R$ 10,000 - approximately USD 460 to USD 2,400. Judges often establish these values arbitrarily, according to the caused damage in each case, stating that the indemnification is based on principles of proportionality and reasonability, and that it has an educational purpose.

As an example of the above, the Superior Court of Justice ("STJ") upheld a decision issued by Minas Gerais State Court, which granted R$ 8,000 (approximately USD 1,800) to a consumer due to the storage of his personal data in the defendant's database, without his consent or prior knowledge[8]. According to STJ, the defendant should have previously informed the plaintiff about the storage of his data, its purposes and the identity of the entity responsible for the management of the information, in order to enable the enforcement of the consumer's right to rectify his data if necessary (Article 43, paragraph 2nd of the CDC) and comply with the dispositions of Law 12.414/2011, which disciplines the creation and consult of databases about credit history.[9]

In another case, decided by the State Court of Rio Grande do Sul, the City Hall of Montenegro was ordered to pay moral damages to public workers due to a partnership with the Brazilian financial institution named Caixa Econômica Federal that resulted in the sharing of personal data with third parties, without the data owners' consent.[10]

According to the Court, the illicit act was not caused by the partnership with Caixa - which also involved the sharing of the public workers' personal information - because it was based on a discretionary act of the Public Administration aimed at adapting the needs of its own organizational structure. The issue was deemed to be the sharing of the citizens' data, collected by the City Hall and transferred to Caixa, to a third party, who was given an undue access to this information and violated the right to privacy foreseen in the Federal Constitution.

For the breach of the public workers' data, the City Hall of Montenegro was requested to pay R$ 3,000 (approximately USD 691), for each of the complainants, due to the moral damages caused.

**1.3.The Brazilian scenario during LGPD's vacatio legis**

In 2019, IBM Security in association with Ponemon made available the Cost of a Data Breach Report[11], which was conducted in 16 territories[12], and was based on information from 507 organizations that experienced a data breach between the periods of July 2018 and April 2019. This report defines a data breach as *"an event in which an individual's name and a medical record and/or a financial record or debit card is potentially put at risk, either in electronic or paper format"* and depicts a concerning scenario among Brazilian organizations and the incentives towards data protection before the entry into force of the LGPD.

According to its findings, Brazil presents one of the lowest averages regarding costs[13] derived from a data breach - approximately USD 1.35 million - which means that organizations in this territory do not bear high financial losses when facing situations of leaked information, if compared to the worldwide average of USD 3.92 million. The differences among countries' averages are expansive, with North American and Middle Eastern organizations burdened with the highest averages, reaching USD 8.19 million and USD 5.97 million, respectively.

As well as presenting one of the lowest average costs per data breach, Brazil occupied the third place in the number of exposed or compromised records - up to 26,523 - above the global average of 25,575. This situation indicates that Brazilian organizations have faced situations of breach of data between 2018 and 2019 in which huge amounts of informationwere unprotected, but have not suffered considerable financial losses. They therefore have less incentive to prevent future data breaches.

The above situation is aggravated by the fact that Brazilian organizations require approximately 361 days to solve a data breach. This constitutes one of the longest "breach lifecycles" in the world. This indicates that, in Brazil, the time between the occurrence of a data breach incident and its containment takes almost an entire year. The average worldwide lifecycle of a data breach in 2019 was 279 days.

These circumstances create great concerns in Brazil regarding the entry into force of a law that is dedicated to personal data protection and which establishes strict penalties for a failure to comply.

"the initial regime... is causing debates over the actual independence of the ANPD from the Executive branch, and its capacity to become a financially independent and impartial entity in the future."

Based on this, the fast approach of the new data protection law enforceability is creating numerous speculations on how the National Data Protection Authority ("ANPD") and the Judiciary will apply the regulations and how agents subject to these norms must adapt their businesses and day-by-day lives to the created standards

## 2. The main characteristics of the Brazilian General Data Protection Law and its similarities to EU's General Data Protection Regulation

**2.1. The generic aspects of the LGPD**

When comparing the GDPR to the Brazilian General Data Protection Law, one of the first observations should be the number of articles - 65 articles when compared to GPDR's 99 articles - and the specificity of its definitions. Despite the attempt of the Brazilian legislator to adapt the local law to the European regulation, the final text does not present complete information on the concepts used and the proceedings provided for, and still relies on further regulation from the ANPD in order to be fully effective.

In general terms, LGPD is based on the GDPR, but does not address its goals properly, leaving several gaps that must be filled in by the ANPD, the Judiciary or further amendments to the law.

For example, the Brazilian law defines personal data as "any information related to an identified or identifiable natural person", which is an identical concept to the first part of GDPR's Article 4 ("Definitions"). However, differently from LGPD, the European regulation went further by explaining what constitutes an "identifiable natural person", providing several examples of data that are subject to its rulings and, therefore, a better understanding to the public[14]. This kind of information would be useful to a Brazilian reality in which companies and individuals are not familiar with terms that are very generic and not often used so far.

Another example of LGPD's gaps and generic terms is Article 18, that provides for the rights of the data subject. Its corresponding section in the GDPR, Chapter 3, describes in detail in each of its articles (from 12 to 23) the rights that are granted to an individual whose data is used by a third party. On the other hand, LGPD lists data subjects' rights through bullet points, without explaining whatsoever the definition or the extension of each right. For instance, the right of access in GDPR by itself has 8 items containing the information that can be requested by a data subject. In the Brazilian law, this right is merely described as "access to data".

Considering the generic aspect of several LGPD's articles, data operators and controllers might not have full knowledge about how to comply with the law until the ANPD regulates its application, and Courts start to render decisions related to its enforceability. This situation could - and should - be primarily solved by a strong structured National Data Protection Authority, which ought to take the lead in regulating and monitoring the new law, considering the expected expertise of its members.

**2.2. The creation of the Brazilian National Data Protection Authority ("ANPD"**

The final text established to the LGPD by Law 13.853/2019 defines the ANPD as a federal public administration's body and a part of the Presidency of the Republic. However, the judicial nature attributed to the authority is described as merely temporary, leaving the possibility of transforming the ANPD in an entity from the indirect federal public administration, acting under a special autarchic regime associated to the President.

Despite the fact that ANPD was granted technical and decision-making independence since its creation, the above cited transformation would be subject to an evaluation from the Federal Executive branch. As a result of this arrangement, the initial regime established for the Authority, dependent to the Presidency, who is responsible for its transformation into an autarchy after its first years, is causing debates over the actual independence of the ANPD from the Executive branch, and its capacity to become a financially independent and impartial entity in the future

The transformation of the ANPD's nature to an autarchy is a highly expected modification, due to the understanding that it would prevent the Authority from issuing regulations and decisions bound to the ongoing governmental views.

"The Brazilian law does present a difference from the GDPR that the local legislators believed would be positive and necessary to the current Brazilian context."

Also, it's important to note that, until April 15, 2020, ANPD was still not structured and had no members appointed by the Presidency, causing an increasing concern over the enforcement of the new Brazilian personal data protection law. Even though Brazil was involved by Covid-19's pandemic situation as from March 2020, LGPD's final text had already been approved since July 2019 and no further action from the Executive branch was observed to address the issue until then. Regardless of entering into force on August 2020 or January 2021, the lack of a structure for the ANPD could cause the new law to become innocuous.

**2.3. The revision of decisions based solely on automated processing**

Despite the above comparison between the Brazilian and European legislations - that points out LGPD's flaws compared to the latter - the Brazilian law does present a difference from the GDPR that the local legislators believed would be positive and necessary to the current Brazilian context.

The initial Brazilian personal data protection bill of law stated that data subjects could object to decisions that affect their interests[15] and were based solely on automated processing. However, on July 8, 2019, Law No 13.853/19 was published, amending the LGPD to veto the requirement that the evaluation of the automated decision should be performed by a human, differently from what is established in the GDPR.

According to the veto, this criterion would violate the public interest, since it would prevent the functioning of new businesses models - such as startups - and impact credit risk analysis of new financial institutions models, creating a negative effect on the credit offerings to consumers (regarding guarantees' quality, the amount of hired credit, price fixing, inflation rates and even local monetary politics).

Nevertheless, it is important to highlight that one of the purposes of this article, both in LGPD and GDPR, would be protecting right's holders from possible flawed and misleading technologies, that could be harming these individuals' rights and interests. The article also aims at empowering citizens against companies, on the one hand, indirectly demanding that these entities provide better and more accurate services.

On the other hand, it could also be pointed out that allowing the revision of automated decisions would not necessarily lead to more transparency of the algorithms due to (a) LGPD's restrictions to the disclosing of business and industrial secrets that could be needed to explain certain automated decisions; (b) the complexity of certain systems to the right's owners understanding; and (c) the unpredictability of algorithms, which might not allow companies to fully understand the reason for a specific decision by their automated system.

**2.4. Penalties**

In regards to LGPD's sanctions, Article 52 presents a list of six administrative penalties that can be applied by the ANPD to entities that process personal data and infringe the law, willfully or not. These sanctions consist of: (a) warnings, establishing a deadline to correct the violation and comply with the law; (b) simple fines, up to 2% of a private company/group/conglomerate's turnover in the last financial report, limited to R$ 50,000,000.00 per violation (approximately USD 9,800,000.00); (c) daily fines; up to the limit established in item b; (d) publishing information about the violation, once it was duly investigated and confirmed; (e) blockage of personal data that was subject to the violation, until compliance to the law; and (f) elimination of personal data that was subject to the violation.

Before the last amendments performed by the President, the Brazilian data protection law presented three additional penalties to infringements: (a) partial suspension of the database correspondent to the infraction for a maximum period of six months, renewable for an equal period, until the correction of the controller's processing activities; (b) full suspension of the data processing activities related to the violation for a maximum period of six months, renewable for an equal period; and (c) total or partial prohibition of activities related to personal data treatment.

These three possibilities were vetoed due to the understanding that they would create insecurity to agents responsible for processing personal data, prevent the use of indispensable databases to numerous private activities, possibly damage the national financial system's stability and affect the performance of public services. In this context, financial institutions were considered one of the biggest concerns, since the suspension of their databases by the ANPD could severely hinder Brazil's economy.

"It was observed that international companies established in Mexico demonstrated a faster and more proactive compliance to the GDPR, than to the local legislation on the matter."

Also, the LGPD partially incorporated the European Law's standards regarding fines, but did not differentiate the applied amounts by the articles and principles violated. This situation causes the Brazilian legislation not to express the level of importance between its provisions, leaving this judgement to the ANPD and its evaluation over the parameters of Article 52, 1st Paragraph[16].

Considering the lack of legal history around personal data protection, the absence of express dispositions regarding the importance of each LGPD article could create a misbalance in the application of fines.

Moreover, an anonymous source informed a national newspaper that the Federal Government expects to collect up to R$ 20 billion (approximately 4 billion USD) in the first year after the Brazilian Law has come into force[17]. Telecom companies and social security entities are among the possible recipients of sanctions. Despite the high number estimated by this source and the disbelief that the ANPD and the Law itself would allow the use of the LGPD for government collection purposes, the discussion regarding the misbalance of the applied fines, either due to the amount or frequency of application, is a valid concern, not only in the administrative ANPD field, but also among the Judiciary.

**2.5. Data Protection regulation around Latin America**

As for the regulation and protection of personal data around Latin America, it is possible to observe that other nations already enforced specific legislations on the topic, which made the adaptation to the new European regulation a simpler transition.

**Mexico[18]**

Mexican legislations on personal data protection are guided by the principles of legality, consent, notice, quality, purpose, fidelity, proportionality and accountability. Despite not being as strict as the GDPR, the Mexican Laws are compatible with the European regulation. As for example, any data owner in Mexico may exercise the rights of access, rectification, removal and objection.

Similarly, this country's legislations state that data controllers must adopt measures that guarantee the proper processing of personal data, which shall comprise, among other dispositions, (a) drafting binding and enforceable privacy policies and programs; (b) implementing a program for training, updating, and raising the awareness of the personnel about obligations regarding protection of personal data; (c) implementing a procedure to deal with data protection risks generated by new products, services, technologies and business models; (d) periodically reviewing the security policies and programs to determine the required modifications; (e) establishing procedures to receive and respond the questions and complaints of data subjects; (f) establishing measures to trace personal data[19].

The local regulations also provide a list of actions that must be carried out in order to comply with the obligation of creating measures to protect personal data, such as: (a) collecting and drafting an inventory of personal data and processing systems; (b) determining the duties and obligations of who processes personal data; (c) carrying out a risk analysis of personal data processing focused on identifying dangers and estimating risks; (d) establishing security measures applicable to personal data and identifying those implemented effectively; (e) analyzing the gap between existing and missing security measures; (f) drafting a work plan for implementing the missing security measures; (g) carrying out reviews and audits; (h) training staff members that process personal data; and (i) keeping a record of personal data storage media.

In regard to the practical impacts of the European regulation in Mexico, it was observed that international companies established in Mexico demonstrated a faster and more proactive compliance to the GDPR, than to the local legislation on the matter. Additionally, Mexican higher courts consider the GDPR as a standard and have used its principles to solve cases regarding local data controllers, creating and developing jurisprudence and case law about privacy and data protection.

**Argentina[20]**

Argentina enacted its own personal data protection legislation in 2000 - the Argentine Personal Data Protection Law (Law No. 25,326) - which was later complemented by different lower level regulations. This law aims at providing *"comprehensive protection for personal data held in archives, registers, data banks or other technical means of data processing, whether public or private"*, "to guarantee the right to honor and privacy of individuals" and the access to the information stored, and has very similar dispositions to the GDPR.

"The [Chilean] Bill complies with several GDPR dispositions while adopting a more liberal approach."

The Argentinean legislation also includes as data owners' rights: (a) asking information regarding the existence of files and databases, their purposes and the entities responsible for the treatment of the gathered data; (b) obtaining information about their personal data included in databases (whether public or private); (c) asking for the rectification, update, exclusion or secrecy of their data; and (d) filing for legal action for protection of their personal data (habeas data).

Argentina also demands that databases are registered with the Argentine Agency of Access to Public Information (*Agencia de Acceso a la Información Pública* or AAIP). The AAIP is entitled to impose fines and other penalties in the event of infringement of the local data protection law.

Moreover, the Argentinean Criminal Code contains numerous provisions in order to protect personal data. For example, illegal access to personal data files, and disclosure of information registered in a personal data file or bank whose secrecy is required by law, is considered a criminal offence.

Considering the above, it is important to note that the Argentinean data protection legislation was inspired by former European regulations, in force prior to the approval of the GDPR. For this reason, Argentina still needs to update its internal legislation to the new standards established by the GDPR.

To meet the new European rules, Argentina has become officially part of the *"Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data"* (Convention 108)[21] in 2019 and executed the Additional Protocol, which is currently in the process of approval by the National Congress. The Argentinean Congress is also analyzing a bill of law focused on updating the local personal data protection regulations to GDPR's standards and the latest technical developments.

In the above context, the AAIP has approved Resolution 4/2019, which sets best practices guidelines for the implementation of the data protection legislation. It comprises dispositions such as the following: (a) grant of rights to the access of personal data collected through video surveillance systems, since one's personal image is deemed as part of the concept of personal data; (b) obligation to the responsible for a database to have effective identity validation mechanisms to verify that the individual who gave consent is the respective data owner; (c) addressing of data processing consent from minors, as well as a best-effort rule for data controllers regarding the verification of their parental consent; and (d) determining that biometric data is part of the definition of personal data and it will be considered sensitive data provided its use can result in the discrimination of the respective data subject[22].

**Chile[23]**

In Chile, the main privacy legislation is entitled Privacy Act - Law 19.628 on the "Protection of Private Life and the Treatment of Personal Data" ("DPA").

The DPA states that any person or entity in the private or public sectors may use or disclose personal data (a) for a legal purpose authorized by the DPA or other legislation, or (b) if expressly authorized by the data owner. According to the law, consent must be manifested in writing and will only be valid if the data owner was previously informed about the purpose of obtaining his/her personal data and the potential disclosure of such data to third parties.

In 2017, the local government signed the Privacy and Data Protection Bill ("Bill"), which incorporates data protection standards from the Organization for Economic Cooperation and Development ("OECD"), such as the creation of a data protection agency in Chile. After its approval by the Senate, the Bill awaits its enactment, which it is expected to occur in 2020.

Unlike the DPA, the Bill complies with several GDPR's dispositions while adopting a more liberal approach. Its dispositions are a result of discussions in the local Congress regarding GDPR's standards.

As the Bill has not been enacted yet, other authorities have started to engage in privacy issues as an effect from the GDPR. This is the case of the National Consumer Bureau ("SERNAC") on consumer protection and the Commission for the Financial Market ("CMF") on cybersecurity issues.

"Colombia makes a distinction between public, semi-private, private and sensitive personal data."

Moreover, Chilean companies have already begun to introduce higher levels of privacy standards into their treatment of personal data due to the European legislation. These companies are mostly international entities that have a connection with European citizens or companies, or that have e-commerce webpages or apps that are used by Europeans .

**Colombia**[24]
Colombia also adopted personal data protection legislations before the enactment of the GDPR in Europe - i.e. Laws 1,581/2012 and 1,266/2008. Despite presenting similar dispositions to the European regulation, the Colombian laws are considered to be less strict.

Colombia makes a distinction between public, semi-private, private and sensitive personal data. Public data do not constitute special obligations and can be stored or used by anyone and by any means, as long as its use does not aim at causing harm to individuals, corporations or state agencies. As for private data, it demands previous consent from the owner for its use, storage and sharing, and may only be processed withing the scope of the authorization granted by the rights holder.[25]

Semiprivate data consists mainly of financial data. Its obligations are required especially from Credit Report Bureaus, which must follow the same obligations established for private data and, also, (a) assure that all single Credit Report Bureau is incorporated in Colombia; (b) create a customer service area within the company; (c) update the information stored every 10 business days; and (d) adopt proper and more efficient security systems and protocols.

The use of sensitive data in its turn demands prior consent from the right's holder, unless the information is used for: (a) the right holder´s protection, in the event he/she is legally or physically unavailable to consent to it; (b) historic, scientific, or statistical purposes - without identifying the right's holder identity; (c) purposes associated with his/her legal defense.

In addition, the owner's authorization is not previously required for the use of sensitive data by NGOs for religious, philosophical or political purposes, as long as all necessary measures are taken to ensure the security of the personal information. In this scenario, the right's holder needs to be affiliated to the organization that is using the data. On the other hand, this exception does not entitle NGOs to publicly disclose the sensitive data.

In Colombia, general data owners in general have the right to (a) acknowledge, update and rectify their personal data; (b) request evidence of their consent to treat their personal data; (c) be informed about the use of their personal data; and (d) revoke their authorization to treat personal data.

Moreover, Colombian legislations state that personal data may be transferred abroad, as long as the country where the data is being transferred to has at least the same standards of protection that the country has.

Finally, differently from the GDPR, it is understood in Colombia that valid consent might be obtained by any means that allows subsequent consultation. The European regulation states that consent shall be given by a statement or by a clear affirmative action, which indicates a more clear and direct way of controlling the obtainment of consent.

Nevertheless, the GDPR has considerably impacted personal data protection in Colombia since it is now a reference for standards of good practices. As of Colombian Companies, given the extraterritorial application of the GDPR, some have updated their privacy policies, especially those that trade goods and services in the European Union, or that treat personal data from EU citizens.

"Brazilian entities, from the public and private sectors, need to start organizing their priorities around personal data protection."

## 3. Future expectations on personal data protection in Brazil

By the time this article was written, the Brazilian General Data Protection Law was supposed to enter into force in August 15, 2020, causing great concern over the gaps and uncertainties described above.

The application of the law in Brazil, though, presents great importance for other countries, especially among the European Union, as a demonstration of the Brazilian efforts to update internal regulations to the current international regime on personal data protection and privacy matters. Ideally, the ANPD should be duly organized within the remaining period of time until August 2020 (or January 2021, if Bill of Law 1.179/2020 becomes effective), in order to ensure the correct enforcement of the new law.

Despite the lack of preparation not only from private companies, but also public institutions, the delay in the application of the LGPD does not seem appropriate if it's not motivated by the need for a structured ANPD. Brazil has delayed discussions about the creation of a legislation focused on personal data for too long. Its current laws are outdated in relation to the international scenario, notably nowadays when personal data protection rules become essential in a context where sensitive data - such as medical records - are in the spotlight due to Covid-19.

As observed from the Latin America section of this article, other countries have been incorporating and developing personal data protection laws and regulations for years or decades. Despite the fact that most of them are not (fully) as strict as the GDPR, it is possible to state that it is less complex for a nation that already faces regulations on the protection of personal information to adapt its standards to the new European rules, than a country - such as Brazil - to create a brand new law on a scarcely discussed matter.

Considering the above, Brazilian entities, from the public and private sectors, need to start organizing their priorities around personal data protection. The costs of compliance might be high for some companies - especially during and after Covid-19's quarantine - and the period of adaptation is short, but LGPD represents a crucial and indispensable legislation in the country, especially regarding the tech sector.

In the meantime, the Brazilian Executive should be rushing to correctly structure the National Data Protection Authority, in order to achieve a reasonable enforcement of the law at first instance, as well as to show credibility before foreign countries. Considering the current political situation in Brazil, a personal data protection law created just to appear to comply to EU's GDPR would not contribute to the Brazilian image worldwide, foreign investments in the country or - which is highly concerning - the international transfer of personal data among nations - an essential part of numerous profitable businesses in Brazil and abroad.

[1] *This article was written 1n April2020, during discussions among the Brazilian Legislative branch about Bill of Law 1.179/2020, which aimed at extending LGPD' vacation legis until January 2021, due to the quarantine caused by Covid-19 in Brazil.*

[2] *CRFB/88 - Article 5 - X - the rights to privacy, honor and image are inviolable, being ensured the right to compensation for material or moral damages arising from their violation;(…) XII - the secrecy of correspondence and telegraphic communications, data and telephone communications shall be inviolable, except the latter by a court order, in the circumstances and in the manner established by law for the purposes of criminal investigation or prosecution.*

[3] *On July 2, 2019, the Brazilian Senate has approved a proposal to amend the Federal Constitution ("PEC") that aims at including the protection over personal data in the list of fundamental rights and guarantees. In addition, the PEC intends to grant exclusivity to the Union for legislating on protection and treatment of personal information.*

[4] *Procon imposes fines on Google and Apple due to face images editing app, https://www.conjur.com.br/2019-ago-30/procon-multa-google-apple-aplicativo-edita-imagens-rosto.*

[5] *The resemblance entails the offer and purchase of a service/product and the differences and unbalances between the parties in terms of financial power and knowledge.*

[6] *Marco Civil - Article 3 - The discipline of Internet use in Brazil has the following principles: II - protection of privacy; III - protection of personal data, as provided by law;(...)*

[7] *Uber, Netshoes, Facebook, Inter Bank and C&A were a few of the main cases of data breach only in 2018. Available at: https://www1.folha.uol.com.br/tec/2019/01/relembre-os-principais-vazamentos-de-dados-de-brasileiros-em-2018.shtml.*

[8] *Superior Court of Justice, Special Appeal No 1758799, Judge Nancy Andrighi, Date of trial 11.12.2019.*

[9] *The Superior Court also stated that "The mere fact that the data discussed in this case consists of information usually provided by consumers themselves when purchasing anything in the commerce, does not discharge the responsibility of the owner of such database (to inform the individuals about the sharing of their information with third parties), considering that when the consumer buys something, he/she is not implicitly or automatically authorizing the seller to announce his/her information to the market; (when the consumer provides information on a purchase) he/she is merely complying to the requirements for fulfilling the purchase, between only two parties, trusting to the supplier the protection of his/her personal data.(…) Similarly, the fact that someone publishes personal information on a social network does not imply consent to the users that access that content, to use their data to any other purpose, especially for financial means."*

[10] *State Court of Rio Grande do Sul, Civil Appeal No 71008884462, Judge José Ricardo Coutinho Silva, Date of trial 10.15.2019.*

[11] *Available at: https://databreachcalculator.mybluemix.net/?_ga=2.6374450.124598519.1584448911-782171641.1584448911.*

[12] *United States, India, the United Kingdom, Germany, Brazil, Japan, France, the Middle East, Canada, Italy, South Korea, Australia, Turkey, ASEAN, South Africa, and Scandinavia.*

[13] *"How do you calculate the cost? To calculate the average cost of a data breach, we collected both the direct and indirect expenses incurred by the organization. Direct expenses include engaging forensic experts, outsourcing hotline support and providing free credit monitoring subscriptions and discounts for future products and services. Indirect costs include in-house investigations and communication, as well as the extrapolated value of customer loss resulting from turnover or diminished customer acquisition rates." - 2019 Cost of a Data Breach Report.*

[14] *Article 4 - (1) - 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;*

[15] *Including personal, professional, consumer and credit profiling, or aspects of their personality.*

[16] *(a) the scale and nature of the infringements and personal data affected; (b) the infringer's good faith; (c) the advantage obtained or intended by the infringer; (d) the infringer's economic status; (e) recidivism; (f) the amount of damage; (g) the infringer's cooperation; (h) the repeated and proven adoption of internal mechanisms and procedures capable of minimizing the damage, aimed at the protection and adequate treatment of data, according to the provisions of item II of the 2nd paragraph of Article 48 of the LGPD; (i) the adoption of a good practices and governance policy; (j) prompt adoption of corrective measures; and (k) the proportionality between the scale of the violation and the the applied penalty.*

[17] *O Globo, "Quem vai salvar o Rio?", https://oglobo.globo.com/brasil/quem-vai-salvar-rio-1-24095817.*

[18] *Contribution by Luis Mario Lemus Rivero, Esq., Calderon & De La Sierra Attorneys at Law.*

[19] *It also includes (g) establish an internal and external supervision and monitoring system; (h) dedicate resources for implementing the privacy programs and policies; (i) develop mechanisms to comply with privacy policies and programs, as well as sanctions for a breach thereof; (j) establish measures to protect personal data, specifically, technical and administrative actions that will allow the data controller to ensure compliance with the principles and obligations established by the Law and the Regulations.*

[20] *Contribution by Marcelo García Sellart, Esq., law firm Berton Moreno Ojam.*

[21] *This convention focuses on the protection of personal data, considering the growth of the technological development that allows automatic processing of data. Argentina was the third Latin American country to join the convention, after Mexico and Uruguay.*

[22] *Resolution 4/2019 also states that if the responsible for the database decides based solely on automatic processing and that processing cause harmful effects on the data subject, the database controller must provide the latter with an explanation about the logic applied in that decision. In addition, this regulation establishes additional guidelines for*

*applying rules about data dissociation. If it takes disproportionate or impractical measures or deadlines to achieve the identification of a person, that data will not be deemed as related to a "determinable person".*

[23] *Contribution by Felipe Claro, Esq., law firm Claro & Cia.*

[24] *Contribution by law firm Cavelier Abogados.*

[25] *The use of private data requires compliance to numerous obligations, such as (a) the right's holder consent to the use of its personal data (through voice or writing) must be always held and stored; (b) data can´t be publicly disclosed, unless authorized by the right's holder; (c) right's holder must be informed of the identity of any person in charge of storing or using the data, and of any changes in the identity of this person; (d) all information comprising the data, must be updated or amended whenever his/her owner requests it; (e) reports regarding the use of the data must be delivered to the request of the right's holder; (f) the right's holder must be notified in case of any breach of secrecy of the data; (g) the right's holder shall be informed of his/her rights.*