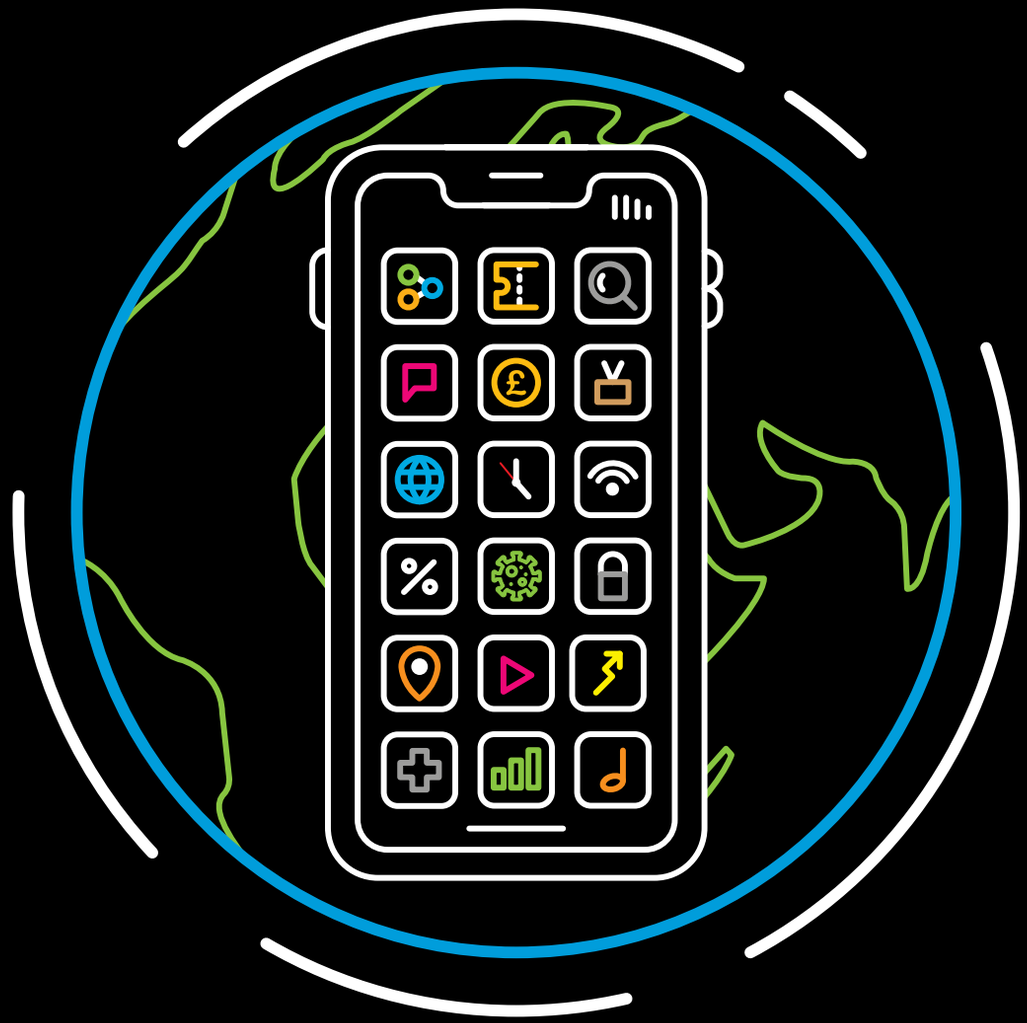
INTERNATIONAL ASSOCIATION OF ENTERTAINMENT LAWYERS

Nationalism vs Globalism: Regional and Transnational Legal Issues Reshaping the Entertainment Industry.

Edited by William Genereux & Marijn Kingma



Message from the President: Jeff Liebenson

Welcome to our 2021 IAEL book. The topic of Nationalism vs Globalism has exceeded my expectations, even covering issues arising from working during a pandemic.

We can only hope that the devastation the pandemic has brought across the globe will subside and we will once again meet in France in next June for our annual IAEL meeting during Midem.

The ongoing relevancy of the topics in the book reflects the world we live in today as the rise of nationalism separates countries and globalization brings them together. 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.

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 this book. Our contributors from around the world illuminate these developments from their own perspectives which inform their articles.

Thanks to Duncan Calow and Marcel Bunders for your continued support, guidance and humor with respect to the many adversities we have weathered these past two years.

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 IAEL meetings with members from around the world enjoying our different cultures and coordinating our common interests.

We hope this book furthers that spirit, 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 we had our last IAEL General Meeting in June 2019, we could not have foreseen we would not be able to come together in Cannes for the next two summers – or that as a result of a pandemic we would not be publishing the entire book until well into 2021. We also could not have foreseen how relevant the topic of our book would turn out to be. Over the last year and a half we have been on a global rollercoaster ride and it has become more clear than ever that we do not live in separated worlds, and that national borders do not mean anything when push comes to shove. We have also learned that global efforts are needed to solve global problems. Many countries came together to find the vaccines needed to get us out of this situation. The COVAX program is trying to provide global equitable access to vaccines so that not just some countries, but the whole world can hopefully return back to normal soon. Hopefully we will learn from this experience for that other, even more pressing, global emergency: climate change.

Although it was a difficult decision to postpone the release of our book last year, we believe it was the right decision. It gave us the opportunity to include additional contributions dealing with the impacts of the pandemic on the entertainment industry and take a look at how to move forward. The chapters that were written last year have been updated, resulting in a comprehensive publication that we believe was worth waiting for.

The chapters in this year's IAEL book explore the longstanding conflict between nationalism and globalism as it relates to the entertainment industry. Originally we had intended to use the term "globalization" in the title rather than globalism. That probably would have been more correct, insofar as globalization is a word used by economists to describe a process by which businesses or other organizations develop international reach or increase the international scale of their operations. Globalism, on the other hand, tends to be more of a raw, emotional, political concept. It describes a potential threat that can be rallied-against. It's often rejected by nationalists, conspiracy theorists and indeed anyone who might be content to sit in their own backyard and let the rest of the world be damned. It's used often in a defensive way – to describe existential threats that are perceived to have been created by others, like having rules or market forces emanating from outside our own borders that nevertheless come to affect us.

We decided to go with the more difficult word, globalism, because it more accurately describes the zeitgeist of our times. Our entertainment industry already is global, and international trade, which is what globalization is all about, has been occurring and disrupting markets since at least the early days of spice trading thousands of years ago. Now of course the Internet allows us unprecedented new types of access to foreign markets and the promise of having our services and products seen, heard and used by countless millions of others. This development has moved up a gear due to the pandemic. But here's the thing, there are a lot of vested interests that get in the way. The forces of disruption invariably leave footprints across the backs of incumbents. There usually are winners and losers, and even the venue where this all happens – our planet Earth – becomes a stakeholder as we take environmental issues into consideration. The discussion about what's best for the entertainment industry moving forward becomes nuanced, because it's not simply about changes that make things cheaper, faster or most transparent. Folded into the discussion are issues about people, culture, autonomy, stability, flexibility, privacy, freedom and sexuality. The tension between all these forces is beguiling. It makes for interesting reading but leads to much deeper conclusions. One region or territory might want to defend its culture from being diluted by outside influences, yet might want that same culture to find an audience abroad. A territory or region might enact laws that purport to have transnational reach, yet this might directly encroach on the sovereignty of others. Our willingness to embrace change is tempered with fears of losing the status quo. Ultimately, these are

all political issues laced with policy considerations that demand to be understood.

The 2020-2021 IAEL book examines an array of regional and transnational forces that currently are shaping the entertainment industry. Chapters have been subdivided into three major categories, as shown in the table of contents. 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.

The first part of the book focuses on regional issues and differences. This part includes articles on sometimes underexposed but increasingly important markets: India and Nigeria. A contribution from Italy focuses on documentary films and cultural heritage, and the viability of specific Italian legislation in the light of Europe's DSM Directive. There are several articles about major legislative developments in the U.S. and the EU, including the U.S. Music Modernization Act and the EU Audiovisual Media Directive. A comparative contribution from three of our authors describes the limitations and exceptions to copyright in three major territories: the EU, the U.S. and Asia.

The second part of the book shows that regional developments can have global consequences. The GDPR, for example, has left its marks all around the world as countries are adapting their data protection legislation to keep up with Europe's strict rules. The infamous article 17 of the EU DSM Directive is bound to have an impact on the rest of the world. These global influences of regional legislation are discussed in this part of the book. This chapter also looks at the global impact of new technology and new industry economics. Important issues that are discussed include licensing in the age of globalization, how to deal with aggregators, and new types of platforms. And let's not forget something that we all have in common: paying taxes. A contribution from the Netherlands looks at the influence of globalization on international tax principles. Finally, we have an article that focuses on jurisdiction of U.S. courts. Under what circumstances can a non-U.S. entity be hauled into a U.S. Court thousands of miles away to defend itself under United States law?

The third part of the book takes a look at some of the broader social and environmental issues of our current and future world. A contribution from Denmark discusses the changing expectations for artists as global role models. Another article looks at the (im)possibility to regulate fake news and political advertising on social media platforms. We also have a very helpful contribution on transgender music artists and the legal issues they encounter. We are also very pleased to have an article on what is no doubt the biggest challenge of our times: global warming. And then there are pandemic-related chapters that we never thought we'd be writing about. They are intended to provide useful information. There's information on data protection laws and privacy from the perspective of several different global regions, and there's information on how the pandemic has affected contractual relations. We also have chapters looking at the effect of the pandemic on future of the entertainment market, such as the acceleration of the shift to streaming and the changed relationship between brands and customers. As the global entertainment industry becomes more entwined, we believe these topics are instructive for everyone in all regions.

We would like to thank IAEL's president Jeff Liebenson for his time, effort and leadership as we've planned, changed our plans, planned again and finally executed on the making of our book. 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, diligence and flexibility. A lot of energy that could have been directed toward remunerative, billable work instead has been gifted to us all, so that we can see the issues in their chapters through their specialists' eyes. Without the generosity of all the contributors this book could not have happened. Thank you everyone.

Finally, to quote Vera Lynn who passed away last summer at the respectable age of 103: we'll meet again.

William Genereux & Marijn Kingma

The Brazilian General Data Protection Law and the Rise of a New Era of Privacy Standards

Authors: Marcelo Goyanes & Leticia Carneiro

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 two co-editions 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 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. Most of LGPD's dispositions became effective in September 18, 2020[1], after several postponements and modifications in its text performed by the National Congress and the former and current Presidents between 2018 and 2020, as well as eight years of discussions of the Bill of Law in the Brazilian Legislative branch.

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 addresses regulation on 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 is a highly regarded right, subject to indemnification

"Despite the understanding that personal data is protected by the Constitution since 1988, it required a specific regulation in order to fully secure the respect to citizens' information"

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 required a specific regulation in order to fully secure the respect to citizens' information, as well as address the complexity of the matter.

In this regard, the 1990's Consumer Protection Code ("CDC") directly mentions the importance and protection of personal data, being used as grounds in the enforcement of data protection cases involving consumerist relations and service providers in general, including situations around access and Internet application providers[4].

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. 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 described as a principle and right separated from the protection of privacy[5]. This change was an indication of the need to have a proper law to regulate the use of personal information in Brazil.

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

Before the enactment of LGPD, the enforcement of personal data protection hadn't reached the local courts in a wide range of cases, despite several data breaches reported by the media[6]. Instead, the case law was usually limited to credit scoring and other cases regarding consumerist's relations based on the application of the CDC.

Courts were often concerned about securing individual´s rights to access the information gathered by service providers, as well as with imposing fines to frauds committed due to the non-authorized use of consumers' personal information by third parties. However, the application of the CDC is restrictive to its purposes, as it cannot be considered a specific legislation on personal data protection.

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 ranged between R$ 2,000 and R$ 10,000 - approximately USD 365 to USD 1,800. Judges often established these values arbitrarily, according to the caused damage in each case, stating that the indemnification was based on principles of proportionality and reasonability, and that it had an educational purpose.

"As to possible effects from the Covid-19 pandemic in its results, the report presented findings indicating that 54% of the analyzed organizations instituted a "home office" system, due to the disease"

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 1,460) to a consumer due to the storage of his personal data in the defendant's database, without his consent or prior knowledge[7]. 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.[8]

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.[9]

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 550), for each of the complainants, due to the moral damages caused.

1.3. The Brazilian scenario during LGPD's vacatio legis

In 2020, IBM Security in association with Ponemon made available their newest Cost of a Data Breach Report[10], which was conducted in 17 territories[11], and was based on information from 524 organizations that experienced a data breach between the periods of August 2019 and April 2020. 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.

According to its findings, Brazil presents one of the lowest averages regarding costs[12] derived from a data breach – approximately USD 1.12 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 3.86 million. The differences among countries' averages are expansive, with North American and Middle Eastern organizations burdened with the highest averages, reaching USD 8.64 million and USD 6.52 million, respectively.

The above situation is aggravated by the fact that Brazilian organizations require approximately 380 days to solve a data breach, consonant to the average worldwide. This indicates that, in Brazil, the time between the occurrence of a data breach incident and its containment takes more than an entire year.

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

As to possible effects from the Covid-19 pandemic in its results, the report presented findings indicating that 54% of the analyzed organizations instituted a "home office" system, due to the disease, and 76% of participants understood that this system would increase the time period for the identification and containment of data breaches. Also, 70% of the report's participants alleged that home office would increase damages from such data breaches.

Based on the above, there are numerous speculations on how the National Data Protection Authority ("ANPD") and the Judiciary will apply LGPD's regulations to protect citizens' personal data and how agents subject to these norms should adapt their businesses and day-by-day lives to the created standards, in order to assure the enforceability of the law.

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[13]. 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

"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."

modification, due to the understanding that it would prevent the Authority from issuing regulations and decisions bound to the ongoing governmental views.

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 current President believed would be positive and necessary to the Brazilian context.

The initial Brazilian personal data protection bill of law stated that data subjects could object to decisions that affect their interests[14] and were based solely on automated processing. However, on July 8, 2019, Law No 13.853/19 was published, amending 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 before companies, 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 relation to the 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 9,200,000.00); (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.

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[15].

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.

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

Mexican legislations on personal data protection legislations 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[16].

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.

Regarding 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

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 Argentinean legislation 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.

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[17].

Chile

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"). It 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.

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.

In this regard, other Chilean 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.

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

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

"Despite the abovementioned scenario, the enforcement of LGPD in Brazil continues to be contested for several reasons, such as by the delay of the National Authority to start performing its functions as stated in the law, regarding its regulatory activities, especially after the discovery of the biggest data breach in Brazil's history, in January 2021"

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 don't 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 to its use, storage and sharing, as well as can only be processed within the scope of the authorization granted by the rights holder.[18]

Semiprivate data is constituted manly 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 on 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 to 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 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.

Also, 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.

3. Future expectations on personal data protection in Brazil

The Brazilian General Data Protection Law has finally become effective on September 18, 2020, after an intense period of discussions on whether it would be once again postponed by the National Congress. Since then, ANPD's members have also been appointed and the law is already being directly applied by the national courts.

Despite the abovementioned scenario, the enforcement of LGPD in Brazil continues to be contested for several reasons, such as by the delay of the National Authority to start performing its functions as stated in the law, regarding its regulatory activities, especially after the discovery of the biggest data breach in Brazil's history, in January 2021.

"...the events of these initial months after the law became effective unfortunately perpetuate the concerns on the actual effectiveness of this new legislation in Brazil. "

This breach has exposed a large and diverse amount of personal data from 223 million people in the country, including deceased citizens, members of the Supreme Court and President Jair Bolsonaro. Until this article was written, on January 2021, ANPD has requested the Brazilian Federal Police to open an investigation in order to determine the source of the data breach, which is unknown so far, however, no other action has been observed from the authority up to this moment.

In addition, it is possible to identify some critics of the initial application of the law by a part of the Judiciary, considering, for example, the apparent inadequate understanding of lower courts towards the legal fundaments for the processing of data. The consent of the data owner seems to be receiving a questionable focus in judicial decisions, as if it were the only or most important fundament in LGPD for the treatment of personal information.

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 and apply a brand new law on a scarcely discussed matter.

There is great expectation on ANPD's actions from now on, as it should occupy a fundamental role in guiding the country, its citizens, and public and private entities towards a more protective and organized system regarding personal data. The enforcement of LGPD is being constantly monitored by several agents in the country, including scholars, and, therefore, the events of these initial months after the law became effective unfortunately perpetuate the concerns on the actual effectiveness of this new legislation in Brazil.

[1] *Articles 52, 53 and 54 of LGPD, regarding the application of administrative sanctions by the Brazilian National Data Protection Authority, shall only become effective on August 1st, 2021.*

[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. Available at: https://www.conjur.com.br/2019-ago-30/procon-multa-google-apple-aplicativo-edita-imagens-rosto.*

[5] *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; [...]*

[6] *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.*

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

[8] *The Superior Court also stated that "The mere fact that the data discussed in this case is constituted of information usually provided by consumers themselves when purchasing anything in the commerce does not excludes 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 in the market; (when the consumer provides information on a purchase) he/she is merely complying to the requirements to the fulfilling of the trade, between only two parties, trusting to the supplier the protection of his/hers personal data. [...] Similarly, the fact that someone publishes a personal information in a social network does not imply consent, to the users that access that content, to use their data to any other purpose, especially to financial means."*

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

[10] *Available at: https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/pt/pdf*

[11] *United States, India, the United Kingdom, Germany, Brazil, Japan, France, the Middle East, Canada, Italy, South Korea, Australia, Turkey, ASEAN, South Africa, Scandinavia and Latin America (Argentina, Chile and Colombia).*

[12] *"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." - 2020 Cost of a Data Breach Report.*

[13] *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;*

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

[15] *(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.*

[16] *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.*

[17] *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".*

[18] *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.*