FUNDAÇÃO GETULIO VARGAS

ESCOLA DE DIREITO FGV DIREITO RIO

GRADUAÇÃO EM DIREITO

KEVIN E. W. B. CATTLEY

LGPD: A COMPARATIVE ANALYSIS OF A NEW LAW IN SHIFTING PARADIGMS

Rio de Janeiro, December/2020.

FUNDAÇÃO GETULIO VARGAS

ESCOLA DE DIREITO FGV DIREITO RIO

GRADUAÇÃO EM DIREITO

LGPD: A COMPARATIVE ANALYSIS OF A NEW LAW IN SHIFTING PARADIGMS

Written by KEVIN CATTLEY

Projeto de Trabalho de Conclusão de

Curso apresentado à FGV DIREITO RIO

como requisito parcial para obtenção do

grau de bacharel em Direito.

Comissão Examinadora:

Nome do Orientador: Professor Dr. Evandro Menezes de Carvalho

Nome do Examinador 1: Professor Dr. Álvaro Palma de Jorge

Nome do Examinador 2: Professor Dr. Luca Belli

Assinaturas:

Professor Dr. Evandro Menezes de Carvalho _____

Professor Dr. Álvaro Palma de Jorge _____

Professor Dr. Luca Belli _____

Nota Final: _____

Rio de Janeiro, ___ de dezembro de 2020.

PLEDGE OF ORIGINALITY

I, KEVIN CATTLEY, as a law graduate student at the FGV DIREITO RIO Law School, declare, for due purposes, that the Course Completion Work presented in the annex, a necessary requirement for obtaining a bachelor's degree in Law from the FGV DIREITO RIO, is fully in accordance with the original technical, academic and scientific criteria. In this sense, I declare, for due purposes, that: The referred TCC was prepared with my own words, ideas, opinions and valued judgments, therefore not consisting of PLAGIARISM, for not reproducing, as if they were mine, thoughts, ideas and words of others; Direct citations of other people's works, published or not, presented in my TCC, are always clearly identified in quotation marks and with the complete bibliographic reference of their source, according to the rules established by FGV DIREITO RIO. All series of small citations from several different sources were identified as such, as well as long citations from a single source were incorporated with their respective bibliographic references, as I was duly informed and advised about the fact that, otherwise, they would constitute plagiarism. All abstracts and / or summaries of other people's ideas and judgments are accompanied by an indication of their sources in their text and they are included in the bibliographic references of the TCC, as I was duly informed and advised about the fact that non-compliance with these rules could lead to allegations of fraud. The Professor responsible for the orientation of my course conclusion work (TCC) presented this declaration to me, demanding my commitment not to practice any acts that could be understood as plagiarism in the elaboration of my TCC, reason why I declare to have read and understood all of its content and submitted the attached document for appreciation by the Fundação Getulio Vargas as a result of my exclusive work.

Date: 30/11/2020

Kevin E.W.B. Cattley

Table of Contents:

Contents

Acknowledgements**:**

I give my thanks for Cristina, for a decade-long stream of support and motivation, making every victory worth double.

For raising me and withstanding my shenanigans, I thank my parents and siblings, respectively, who have supported me in all my endeavours.

For the inspiration they have provided me, I thank my grandparents. In special, I salute my late grandfather, and the exemplary service he provided for his family and country.

I would also like to thank the university, for all it has provided me.

Within FGV, I am thankful to Professor Joaquim Falcão, who gave me the opportunity to work with him, helping me further my interest in law and technology.

Particularly, I would like to thank Professor Thiago Bottino, for being a great source of comfort and guidance during my time at FGV.

Moreover, I wish to thank Professor Evandro Menezes de Carvalho, for the trust he places in me, of which one can guarantee reciprocity.

For fuelling my interest in the subject of data protection, I would thank Professors Luca Belli, Álvaro Palma de Jorge and Ivar Hartman, whose classes I could not have gone without.

Finally, I thank my friends, who have always endeavoured to stand by my side.

FGV DIREITO RIO

“It is a capital mistake to theorize before one has data.”

Sherlock Holmes

RESUMO:

Este artigo busca fazer uma análise crítica da LGPD, desmontando alguns de seus principais componentes e comparando-os e contrastando-os com o GDPR da União Europeia. o Regulamento Geral de Proteção de Dados. Nesse esforço, a pesquisa feita tenta contextualizar os sucessos e fracassos encontrados na legislação brasileira de proteção de dados. Diante disso, o objetivo primário deste artigo é discutir se a LGPD é, teoricamente, melhor do que sua principal contraparte internacional – o GDPR. Secundariamente, o presente trabalho tem como objetivo aplicar os resultados encontrados e filtrá-los por uma segunda lente, discernindo se os benefícios teóricos trazidos pela LGPD têm peso no âmbito da praticidade.

PALAVRAS-CHAVE: Proteção de dados; Lei geral de proteção de dados; Privacidade; Regulamento Geral de Proteção de Dados; Sujeito dos Dados; Extraterritorialidade; Oficial de Proteção de Dados; Multas; Vulnerabilidade; Fonte de Dados; Regulamento; Scraping; Armazenamento; Processamento; Novas tecnologias; Tributação; FinTech.

ABSTRACT**:**

This paper seeks to make a critical analysis of the LGPD, by taking apart some of its key components and comparing and contrasting the same to the EU's GDPR, the General Data Protection Regulation. In this endeavour, research is used to help contextualise the successes and failures found within the Brazilian data protection law. Given this, the primary role of this paper is to discuss whether the LGPD is, theoretically, better than its main, international counterpart – the GDPR. Secondarily, this paper aims to take the aforementioned findings and filter them through a second lens, discerning whether the theoretical benefits brought upon by the LGPD have weight in the realm of practicality.

KEYWORDS**:** Data Protection; General Data Protection Law; Privacy; General Data Protection Regulation; Data Subject; Extraterritoriality; Data Protection Officer; Fines; Vulnerability; Data Source; Regulation; Scraping; Storage; Processing; New Tech; Taxation; FinTech.

Abbreviated Terms:

LGPD	Lei Geral de Proteção de Dados
GRPD	General Data Protection Regulation
BRICS	Brazil, Russia, India, China, and South Africa
DPO	Data Protection Officer
CTS	Centro de Tecnologia e Sociedade
CDC	Código de Defesa do Consumidor
ANPD	Autoridade Nacional de Proteção de Dados

Methodology:

In making a critical analysis of the LGPD, one will be looking into the key issues within the law and their effectiveness, or lack thereof, whilst providing one's own personal take on the legal text under scrutiny. The summary of the legal text, as well as of supporting sources would be far too easy to produce, lacking in challenge, as well showing deficiency in creativity. Therefore, one will go a step further, ensuring well-founded reasoning behind the consequences of the legislators' adherence, or failure to adhere, to some of the LGPD's current, global competitors – all whilst contextualising one's arguments to Brazil's reality.

Naturally, the LGPD, domestic laws and global research will be used, as well as foreign laws and treaties – in an effort to flesh out the basis for the arguments provided. Some case studies may also be used so as to exemplify perceived boons and deficits, demonstrating the inner workings and failings of the LGPD, as well as that of arguments provided by fellow researchers.

It is important to reiterate that a summary would be extremely easy to make and not at all useful. The creative process behind problem-solving, however, is what is of true value, allowing for more than the regurgitation of words – meaning one can build upon a given foundation, rather than describing the same from afar. As such, the most pertinent aspects of the research, as they relate to the law, have been selected for purview.

Finally, in dealing with the LGPD, an unofficial, English, version of the same has been used, as provided by the team at Cyberbrics.info[1], whilst a heavily utilised source, hereby referred to as the '*CTS analysis*', can be found here[2].

[1] "The Brazilian General Data Protection Law (LGPD) – Unofficial English Version" Retrieved on the 20th of July 2020.

[2] "Contribuição do Centro de Tecnologia e Sociedade da FGV DIREITO RIO ao debate público sobre o Anteprojeto de Lei de Proteção de Dados Pessoais" CTS, FGV Direito Rio. Retrieved on the 20th of July 2020.

Foreword about the LGPD:

Since it's formation, Brazil has acquired and adopted laws from other countries into its own compendium. From the Brazilian constitution, which borrowed heavily from the United States of America, to the commercial code, which in many ways resembles prior, Italian variants, the laws in Brazil generally suffer a 'copy and a paste' effect – consequentially, not always working as originally intended. Therefore, when it comes to data protection and its laws, it is not surprising that the Brazilian LGPD resembles, in many respects, preceding data protection laws from around the world.

Borrowing heavily from the European GDPR (General Data Protection Regulation)[3], the LGPD aims to better regulate the instances through which data is governed. In doing so, it must carefully dance between two lines – the need for a law which approximates Brazil to global, data protection laws, easing transactions between like-minded states, as well as meeting the necessity for a law which acquiesces to the reality of Brazilian day-to-day operations. In order for the aforementioned to become reality, the LGPD has had to adapt itself to influential regulations, such as the GDPR, whilst retaining the traits most essential to assure that Brazil does not follow through with the recurring mistake of porting over a law riddled with content most inadequately suited to a Brazilian paradigm.

Before delving into the LGPD, the used sources, and the contribution made by FGV's Technology and Society Centre (DIREITO RIO) to the debate in question, a few caveats are also worth mentioning. The first is to reaffirm the need for the law in question. In suggesting that the legal text be amplified or reduced in size or specificity, it goes without saying that the need for a law of this kind is of paramount importance. Where oil once took gold's place, upon the world's centre stage, as a resource of immense value, data is the currency of the present and the future. The acquisition, processing and storage of data must therefore be regulated so as to ensure that the benefits of dealing with this resource are not squandered. Furthermore, from a perspective beyond monetisation, the protection of citizens, in a time where privacy is most volatile, should be a leading concern to governments across the globe.

In promoting this law, and the articles therein, a legitimate effort to address some of these opportunities, as well as potential problems, is being made.

[3] EUR-Lex – 32016R0679 – EN – EUR-Lex. eur-lex.europa.eu. Archived from the original on 17 March 2018. Retrieved on the 20th of July 2020.

Introduction:

With the development of the web, and all within it contained, the issue arose in that data needed to be acquired and organised into something meaningful. With billions of people accessing the internet every day, visiting online stores, commenting on news pieces and more, came the marketable opportunity to turn such loose information into data points and, subsequently, those data points into something more expressive. Moreover, from a legal standpoint, it provided law makers a new challenge – one which shall undoubtedly reign supreme in the age of the internet.

The LGPD, or as it is known in Brazil, the '*Lei Geral de Proteção de Dados*'[4], is the Brazilian attempt at safeguarding its citizens against the goliath of new and emerging technologies. This law attempts to regulate the way in which information is collected, the methods by which it should be processed, as well as the conditions that should apply to its storage. Moreover, it attempts to tackle, in an age of ever-advancing technological innovations, the risks to personal privacy for the general citizenry. Given this, the issues to be tackled should be approached from three perspectives – those of the companies, the citizens and the governments.

When one speaks of the **company** perspective, one has in mind business and profit. The world today is so very different from what it was during its most profit-driven times. Long are the days of tall chimneys and dark, grey clouds, where there is profit without concern and commerce without conscience. Given this, the need for sustainable growth in a new, vibrant and exciting, emerging industry, cannot be understated. It is precisely for such a reason, fully in the knowledge that businesses are comprised by the very citizens who utilise the services and products therein provided, that methods for safely implementing this tech must be found without curtailing the freedoms afforded to citizens of states around the world.

Though a **citizen** may represent the most common denominator in any state, he or she is not without rights. Rights may vary across the board, when comparing country to country or state to state, in most western democracies. The right to privacy and to be treated as an individual endowed with rights, as opposed to a group, subject to a one-size-fits-all approach, reigns supreme[5]. In this pursuit for the right to privacy and for the maintenance of one's very

[4] "LEI Nº 13.709, DE 14 DE AGOSTO DE 2018", LGPD. Retrieved on the 20th of July 2020.
[5] "Universal Declaration of Human Rights". United Nations. Retrieved on the 21st July 2020.

own individuality, the citizens of the world have never been more outmatched. In an unfortunate turn of events, the world finds itself in a trajectory akin to David versus Goliath, and without the joint cooperation of conscience-driven businessmen and women, politically engaged citizens and active governments, one cannot hope to tackle the beast.

When approaching any of the above, it becomes apparent that privacy is not the only thing at stake. When speaking of taxes, one is reminded of Daniel Defoe, who once wrote, "*Things as certain as death and taxes, can be more firmly believ'd*"[6]. This statement, expressed in *The Political History of the Devil*, and made as early as 1726, remains as true then as it is today. Given this, it comes as no surprise that the issue of taxation of data, the world's most treasured commodity, at present, gave rise to concerns within **governments** that their citizens' data was not generating monetarily what it could for the state. When one speaks of the taxation of data, one starts to unfold a great many issues. In this, the matter of data localisation, whether by country, state or municipality, is key.

The issue of citizens either losing out on the profit they are producing , whether this be by not receiving an income from their data or missing out on receiving better products and services, as provided by the state, as a direct result of the taxation of their data, is also of grave concern.

Finally, the bargaining power held by big tech lobbying is vastly unseen by the regular citizen, though it has the power to shape countries in catastrophic ways - from deciding on elections and on legislations, as well as engaging in acts of social engineering.

Given the above, it would be rather unrealistic to expect a law to patch all of the issues stated, affecting all cycles of data and creating some sort of utopia where tech is a useful ally and nothing else. Nonetheless, whether by the work of Samaritans, NGOs or academics, the importance people attribute to the safekeeping of their data has become increasingly more apparent, generating advances in the field. The average citizen of Brazil, Europe and North America[7] has become staggeringly more concerned with the destination of his or her datum[8]. Furthermore, around the world, governments of varying ideologies have started not only to take note of the importance of data and the way in which it is regulated and governed, but also

---

[6] DeFoe, Daniel (1726). The Political History of the Devil, As Well Ancient as Modern: In Two Parts. London: Black Boy in Pater-noster Row. p. 269. Online version available here.

[7] "People Are Becoming More Reluctant To Share Personal Data, Survey Reveals" Forbes. Retrieved on the 21st of July 2020.

[8] "Finally, the world is getting concerned about data privacy." Retrieved on the 21st of July 2020.

taken active measures to protect what they may view as a breach of sovereignty - a direct result of rapid advances in technology without the legislative and judicial momentum necessary to safeguard their geopolitical spheres of influence.

Worthy of mention, without an actual analysis of the merit of governments, their ideologies and espionage efforts, is a hack which took place in July 2019 and resulted in the theft of a Brazilian Minister's personal data, sparking a fire under congress' feet. Shortly after, the senate approved a proposal to amend the Constitution, named PEC 17/2019[9], which would classify **data** protection as a **fundamental right**. This would be added via the altering of art. 5, XII, which defines as "*inviolable*" the confidentiality of correspondence, telegraphic communications, **data** and telephone communications. This proposal awaits final congressional approval, though it could, potentially, add weight to the seriousness with which data is regarded in Brazil, further stoking the fires of the country's latest data protection act.

When analysing the Brazilian case, it is essential to understand the underlying implications that the law may have given the country's culture, the direction in which the judicial branch tends to gravitate towards, as well as how the theory behind legislation, such as the LGPD, suffers or strives in practicality. Factually, Brazil is a very internet-heavy country[10]. Brazilians are amongst the greatest users of internet in the world. Whether it pertains to social media platforms, such as Facebook, WhatsApp as a communication tool, or even video games[11], the fastest growing sector of the entertainment industry, Brazilians are represented within these sectors in great numbers.

Finally, the issue of data protection has never been so poignant for another reason, this being the implementation of 5G technology. 5G technology allows users to transfer data at alarmingly fast rates. Whilst many believe that presidents, Supreme Court justices or even legislators shape the world in which we live in today, one could venture to say that the world is, rather, shaped by new technologies. Whether gunpowder in China[12] or the Elamites and the wheel[13], technology changes the way in which society interacts with itself and with the clay pit that is the world. In this, efforts such as 5G technology will be no different. New and exciting

[9] PEC 17/2019 Retrieved on the 21st of July 2020
[10] "Digital 2020: Brazil". DataReportal – Global Digital Insights. Retrieved on the 21st of July 2020
[11] "Esports in Brazil: Key Facts, Figures, and Faces" Retrieved on the 21st of July 2020
[12] Lorge, Peter A. (2008), The Asian Military Revolution: from Gunpowder to the Bomb, Cambridge University Press, ISBN 978-0-521-60954-8
[13] Tunis, Edwin (2002). Wheels: A Pictorial History. p. 9.

technologies are always being developed and it is up to the world to receive and allow them to grow with the proper incentives and constraints.

Nonetheless, technology has always developed at least a step ahead, if not many more, than legislations. Seeing the effects of new and emerging subsectors of industry, some countries capitalise upon the same – such as Estonia, which considers access to the internet a fundamental[14], human right[15]. In other states, the meaning of internet access and data protection is more profit-driven, such as in the US, where net neutrality remains, to date, a polemic and topical issue[16]. Still, one would be remiss in failing to mention that the concern for the matter of taxation of data has helped propel the issue of data protection forward, giving rise to the regulation of big tech and how companies interact with their clients, turned product.

Finally, other countries, such as Brazil, have had odd, though not unexpected, pressures driving it to the architect's desk, in an effort to design a framework capable of meeting the modern-day, Brazilian reality. By taking and mixing external, political pressures, borrowing from successful data protection legislations, adding a pinch of concern for the taxation of data and a desire to propel the country forward, both in the development of new technologies and infrastructure, Brazil has made its way unto the world stage – and it has chosen the LGPD as its champion.

[14] "Estonia", Freedom on the Net 2013, Freedom House, 2013. Full Report Available here. Retrieved on the 21st of July 2020

[15] "Estonia, where being wired is a human right", Colin Woodard, Christian Science Monitor, Retrieved on the 21st of July 2020

[16] Wyatt, Edward (April 8, 2011). "House Votes Against 'Net Neutrality". The New York Times. Retrieved 21st of July 2020

The Boons:

The very best parts of the LGPD, one might say, seem to stem from the successful adaptations and internalisations of the GDPR, when further expanded upon, concretely. In these scenarios, the law almost transcribes the GDPR in its text and intent, word for word, adding on context and additional information where certain definitions and protections seem the vaguest. Not only that, but when the non-specificity benefits the data subject, there are golden instances within the LGPD whereby the legislator simply decided not to expand upon an idea – which can be a fine thing to do given the context. This is doubly so when one considers that the judiciary in Brazil has a pro-consumer temperament and, up until the LGPD, the term '*consumer*' might as well have been the closest term the country had to define the average data subject.

Personal Data

One of the first challenges for those who wish to study data, and its management, comes with classification. Data, in itself, is a very abstract term and efforts must be made to differentiate the irrelevant data from that of data under the law's protection. Much in the same way an article is written, utilising specific data points to reinforce facts and opinions, huge and random chunks of data hold little to no value to most who obtain them – they must be processed, like oil to fuel or ore to ingots.

In an effort to understand what different types of data there are, one can definitively hit the nail on the head by using the King Midas of terms – 'Personal'. Data and personally identifiable data hold extremely important distinctions in that the former is unimportant, cheap, easily-acquired and largely unprotected, whilst the latter is vital, valuable, often processed and, given implications to privacy risks, sought to be defended by data protection laws.

The GDPR defines personal data as:

"(…) *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."[17]

Evidently, the GDPR is extensively clear as to what this coveted data is, offering the citizens and residents under it's protection a comprehensive umbrella upon which to seek shelter. Meanwhile, the LGPD treats this type of data in more abstract terms, though the legal text still hits the mark. The LGPD refers to **personal data** multiple times as being single or combined strands of data which might identify natural persons or result in individuals being subject to a specific, reactionary, treatment.

Whilst many a lawyer will state that the abstract nature of a contract will benefit the party who drafted it and, whilst in an age of intensive lobbying this could be cause for concer, the vague nature of the LGPD's definition of personal data actually serves to strengthen the protection to those under its enforcement. In using not only the term '**identified'**, but also '**identifiable'** in its text, the LGPD manages to include protection to any data which could be aggregated to another puzzle-piece to identify individuals, without having to pick at smaller traits worthy of protection. Thus, in an equation where 'X' and 'Y' are meaningless, but spell out identifiable data when placed together, both letters in such equation could be considered to be under protection. Though some may find this moot, in an age where technology is rapidly evolving and new data points are being mapped, broad protections are best, as they offer continued, evolving defences – whereas specific legal provisions might find themselves rapidly outdated.

Moreover, it should not go without mention that, whilst the private sector tends to see regulation as an inhibitor to business, as more rules may mean more expenditure on compliance, in this case, one could argue the opposite. There is a good reason as to why many governments across the globe have enacted similar laws to neighbours and trade partners, in areas which include and go beyond data protection. Whether one looks at Europe as an economic bloc, promoting uniformity in many of its laws and member states, or most of the

[17] European Parliament and Council of European Union (2016) Regulation (EU) 2016/679. Retrieved on the 21st of July 2020

BRICS countries[18], which have graciously welcomed GDPR-style laws, one can see the boon in such acts – ease of commerce.

Despite the added care many companies will need to observe when dealing with LGPD-protected subjects, the manner in which the same law conforms with some of its counterparts, such as the GDPR, will certainly increase confidence in those willing and wishing to deal with Brazil. Naturally, shared values will tend to gravitate countries towards one another, in a broad sense, though specific laws which reflect a very serious concern for a treasured right – the right to privacy – may go a step farther. Additionally, in the long run, as countries unify data protection legislations, the overall cost of compliance, for businesses and governments alike, decreases, as less work and time need be expended in order to achieve similar goals.

As one concludes the definition of personal and personally identifiable data, there is yet another addendum to such strings of words which can and should be made – that of '**sensitive personal data**'.

The LGPD strives to protect those under its umbrella in the broadest of terms, yet it also includes additional provisions in an attempt to protect those societally seen as particularly vulnerable to discriminatory practices. It does so via its article 11[19], by further extending its wings to shield personal data concerning ethnic origin, religious beliefs, racial traits, political opinions, health conditions, sexual practices, participation in political organisations and trade unions, as well as biometric and genetic data. In an age where tech moguls speak of microchipping citizens[20], placing a positive spin on an Orwellian-sounding practice, the LGPD creates a small aura of comfort around those who would rather maintain their right to privacy and most personal freedoms, even if at the sacrifice of those nifty, targeted advertisements.

Moreover, a special mention must be made for the treatment of children's data under the LGPD. For those familiar with the extensive nature by which Brazilian law looks to protect children, it should come as no surprise that further, more heightened, restrictions are placed as protection for those deemed as 'children' and 'adolescents'. This comes in the form of further consent, which must be acquired before collecting, processing and storing of data. Where absent, such consent must be acquired from parents or guardians for children, yet not for adolescents. Still, those looking to comply with such a rule will find it mind-bending that the

[18] "10 Countries with GDPR-like Data Privacy Laws" Retrieved on the 21st of July 2020
[19] "LEI Nº 13.709, DE 14 DE AGOSTO DE 2018", art. 11. Retrieved on the 21st of July 2020.
[20] "Elon Musk says there's a chance his AI-brain-chip company will be putting implants in humans within a year." Retrieved on the 21st of July 2020.

LGPD does not define the matter of age classifications very well, nor does the Brazilian constitution, nor the penal or civil code.

Those looking for the defining ages that classify children and adolescents must look the 'Child and Adolescent Statute'[21], which define up to 12 (twelve) years as meaning a child and adolescents as ranging from 12 (twelve) to 18 (eighteen) years of age – yes, those who are twelve, by the code can be both seen as children and adolescents. To add to the mind-boggling nature of the statue, the same claims to be applicable to those between the ages of 18 (eighteen) to 21 (twenty-one). Suffice to say, when litigation starts coming through via the LGPD and the protections it affords children and adolescents, one can only curiously watch from the backbenches as some form of substance is extracted from this mist of confusion – or, to place it gently, this 'requires further clarification'.

Data Subject Rights

When referring to the citizen, resident or person under the protection of the data laws, one could and should simply interchange such terms to 'data subject'. The one whose data is in question is said subject and the rights therein applicable to him or to her are known as the '*data subjects rights*' – a term commonly used in both European legislation and litigation.

When it comes to data subject rights, the GDPR sets forth eight fundamental rights to be upheld, as opposed to the LGPD's nine. Still, one should not become prematurely excited at the notion of the numerical expansion of rights, at the mention of an additional point of protection within the LGPD. In a lukewarm addition to the LGPD, the same has taken eight, almost identical, points from the GDPR and split one of those into two. As implied, such is not a ground-breaking addition to data protection legislation, though it still should, and will, suffer a mention.

The LGPD sets for the **right for a data subject to access their own data** – hence the ability many now possess to request much of what is stored about them on multiple platforms. The reasons behind such a right are multiple, though one can imagine that the slanted nature of the relationship between data subjects and big tech are extreme enough, without the added pressure of such subject having to guess at the cards which comprise the opponent's deck.

[21] "LEI Nº 8.069, DE 13 DE JULHO DE 1990" Retrieved on the 21st of July 2020

Nonetheless, one might even question whether any justification for such a protection is necessary, given that the data originally belongs to the subject. Yet, it is always good to remind oneself that a basic right, such as this one, was not always afforded –showing just how necessary data protection laws can be.

In the case of the processing of a subject's data, the same has the **right to the confirmation of the existence of such processing**. This serves as a powerful reminder to users that their data is undergoing some sort of analysis or modulation and may even afford data subjects the foresight of what might happen to their data, should they share it in a specific location or capacity.

In the possible event that a person is being misrepresented by inaccurate information, data subjects possess **the right to correct inaccurate, incomplete, or outdated information**. This right, afforded to a data subject, though seemingly common sense, can help expedite a process which might otherwise have take lengthy periods of time, as well as multiple requests to the entity displaying or storing the data. Furthermore, the same right can also help in rendering the resort to the judiciary unnecessary or, at the very least, smooth sailing. Moreover, any company or entity large enough to require a Data Protection Officer – something that will be covered later in this paper – will be quick to comply to such a request, perhaps changing the mass usage of Notice and Takedown, more commonly referred to as '*Takedown Notices*', into requests for correction of said data.

When harvested data becomes superfluous, identifiable or excessive in scope or size, the data subject retains the **right to anonymise, block or otherwise delete such data, especially when the same is not being processed in compliance with the LGPD**. This allows the data user who is active to take steps and measures to ensure that his or her data is anonymised and secure. Nonetheless, given the youth of the LGPD, the ambiguity that comes with the usage of words such as 'excessive' is yet to show whether the active or passive poles in the data-driven relationships will stand to lose or profit.

A crucial right for data subjects, when it comes to both the GDPR and LGPD is the **right to portability**. Entire essays could be crafted analysing the necessity for this right, as well as its endless list of benefits for those under the protection of the law. Factually, the ability to generate an express request to transfer one's data, from one product or service provider to another, holds immense implications. If a data subject were beholden to a sole provider or

service, the quality of the same would undoubtedly sink beyond repair. To better visualise the importance of this right, one could draw two, perhaps crude, comparisons.

The first might be to a piece of Brazilian history of interaction with tech, looking back at the introduction of Ubers in the country[22]. The months following the implementation of Ubers in Brazil brought about drastic changes to the way taxis operated. Whilst lawyers and lawmakers attempted to understand the labour repercussions which would come about with the operation of this new service, taxis became cleaner, safer and more readily available for customers around the country. This simple protection, which affords unsatisfied customers the ability to port their data someplace else, has remarkably positive consequences to services provided, generating higher quality for the services in question. In short, more options make for better products and services.

The second comparison that could be made comes from the perspective of empowerment of the data subjects. One of the greatest thinkers of modern times, the late Christopher Hitchens, argued that "*The cure for poverty has a name, in fact. It's called the empowerment of women. If you give women some control over the rate at which they reproduce, if you give them some say, take them off the animal cycle of reproduction (…) not just poverty, but health and education, will increase.*"[23] Though more dramatic in nature, this captures the very essence of what it might mean to have choice, rather than a compulsory, pre-set path. When a data subject stops being a pawn, being moved by big tech in whichever way pleases them, and starts to have the ability to set his or her own course, the power dynamics involved in said relationship become more centred, allowing for data subjects to have some leverage over their own lives. In short, more options make for better choices.

Previously, many entities handling data would request consent to process data and, should a subject agree, whatever was agreed upon might have been fair game for unspecified periods of time. However, the human experience is nothing if not shaped by regret – it is the method by which people adapt their actions and learn from their mistakes. Given this, the **ability to delete personal data which has been processed <u>with the consent</u> of the very own data subject** is essential. It is a hallmark of a sturdy protection, when users are able to flexibly define what data of theirs they wish to shield and, should they cease to provide consent, being afforded the **right to revoke consent** – rights provided by, both, the LGPD and GDPR.

[22] "Uber chega ao Brasil e não quer polêmica". 27/05/2014 27th of May 2014. Retrieved on the 21st of July 2020
[23] Christopher Hitchens , "Christopher Hitchens: Empowerment of Women". YouTube. Retrieved on the 21st of July 2020

Furthermore, in a move akin to the American reading of the Miranda Warning, more colloquially referred to as the '*Miranda Rights*', data subjects are afforded the **right to information on the possibility of denying consent, as well as what consequences might be entailed in so doing**.

Finally, one reaches the GDPR's "Right to be informed", which is, as it sounds, very general. Though this mostly pertains to the data subject being made aware of where and how his or her data is being used, the LGPD made sure to spell the same out, in less abstract terms. Explicitly, the LGPD has turned the GDPR's right to be informed into the data subject's **right to information pertaining to the controller's sharing of data with public and private entities** – a clarification which does not hurt, though does not seem radically different from its point of origin.

One should also note that the newly created agency, the ANPD, charged with enforcement of the LGPD, has since listed another data subject right to the list – **the right to review decisions which utilise personal data to be processed via automated means**. Though the ANPD shall suffer further mention in this paper, one finds criticism to be had in the manner in which this right is extended. Laws, though mutable, are subject to more rigidity and are, therefore, less susceptible to the whims of the few and the winds of transient times. Though providing additional protections for data users is more than often a positive step in the right direction, essential, extended protections should likely be legislatively internalised, rather than depending on agency regulations – the aforementioned being one, such, protection.

As far as variances and resemblances between the GDPR and the LGPD, one would be hard-pressed to find huge distinctions in the rights afforded to data subjects. Given the GDPR's successes since its implementation, it would be difficult to imagine the LGPD falling short in the very similar realm of data subject rights, despite the differences between the Brazilian and European paradigms. Still, as positive as this may be, the motif observed by those looking over the rights listed will note that much of the same require some form of cognisance and/or activeness from the data subject. The subject may be given the information, the right to act, as well as the tools, though the maxim '*Vigilantibus non dormientibus aequitas subvenit'*[24] will always remain true, in that without action, the benefits provided by data protection laws will be a fraction of what they could conceivably become.

[24] Equity aids the vigilant and not those who sleep before their rights.

Extraterritorial Application

Much like the GDPR, the LGPD has extraterritorial application, meaning that the duty to comply with its articles go beyond the geographical limitations of Brazilian territory. Thus, any company looking to deal with the Brazilian market, whether they possess, or not, a branch within Brazil, will need to be in compliance with the LGPD. Moreover, those who deal with personal data, belonging to data subjects found within the country, regardless of their status as citizen, residents, tourist or otherwise, will also be subject to the new data protection law.

Though condemning a person or entity for infringing upon the LGPD and the protections it offers can be quite straightforward, the matter of enforcement abroad can be more complicated. At the very least, holding foreign businesses accountable should remain possible, considering their vested interest in continuing to operate within Brazil. The same can be said for individuals who are found processing data under the scope of this legislation, especially given the slanted balance of power between the average data scraper and the long-reaching arm of the Brazilian government. Nonetheless, when it comes to the enforcement of the LGPD's rules in other countries, one fears, in many cases, despite applicability, matters would be hopeless.

Nonetheless, considering the scope of the LGPD and what it is that it sets out to achieve, the law remains very much on point. Individuals, who were in desperate need of protection, having had to previously make use of subsidiary laws for matters of indemnification, having to press civil or criminal claims using vastly generalised liability laws, are now more adamantly fortified against abuses pertaining to their data and its governance. Furthermore, the ease with which GDPR-compliant businesses and individuals can relate to the Brazilian data protection standards and practices has never been higher – meaning a greater ease for trade, travel, investment, communication and a general proximity over shared values.

The Shortfalls:

In a splendid, almost direct opposite to what constitutes the very best the LGPD has to offer, the bad in the law comes in the form of lack of clarity – especially as relates to obligations and definitions. When a classification is not properly designated, the power rests upon those who draft terms and contracts, who happen to already hold the high ground, to define the undefined. As such, it should come as no surprise that some gaps in the legal text, as pertains to definitions, pose a higher risk to data subjects and should be patched as soon as possible. Moreover, ambiguity as it relates to obligations, will only lead to inefficiency and liability. Most unfortunately, the LGPD is rife with such issues – though the case may be made that it is a new law and, as any new law, it will suffer a heavy crop, resize and recentre before long, hopefully mending many of the significant issues that came with its initial implementation.

Data Protection Officers

In a stride to maintain companies in compliance with data protection laws, both the GDPR and the LGDP have introduced the DPO, or Data Protection Officer. However, here one starts to see where the LGPD and its haziness, whether intentional or not, is lacking.

The GDPR clearly outlines when there is the need for a DPO, firmly regulating the position – as is necessary. Contrarily, the LGPD takes a laxer approach by simply stating, in its article 41, "*The controller shall appoint an officer to be in charge of the processing of data*"[25]. This sentence, though seemingly simple, is rife with issues. Everything it deems to regulate it rather deigns to. It speaks not of the scale of data usage by which DPOs become a necessity, it proceeds to set forth an astonishingly low list of tasks to be accomplished by the DPO, even if the paragraphs which proceed the article attempt to do so in a generalised fashion, it fails to mention any qualifications required of a DPO and further implies that all data processors in Brazil will require a DPO – from Google to your local coffee shop.

The overall vague nature of the LGPD as it concerns DPOs, and the watered-down list of abstract responsibilities unto him or her entrusted, bring little comfort to those critical of the law. Moreover, in a rather bizarre turn, the DPO, within the context of the LGPD, does not

[25] "What is the LGPD? Brazil's version of the GDPR" Retrieved on the 22nd of July 2020

require the position to be filled by a natural person – electing, instead, to allow its attribution to be made before companies, committees or even outsourced groups. Truly, few things are less reassuring than a law which seeks to protect data, but which propels the idea of outsourcing the same duty to mitigate a company's liability. It stands to reason that behind this *laissez faire* approach to vital legislation, which aims to regulate big tech, counterproductivity is often present.

Truthfully, every law made on paper will, more than likely, suffer extensive alterations when confronted with the realities and practicalities of the real world. The LGPD is no exception, though the frequent need for additional clarification is already a common obstacle when interpreting the law in question.

Obligation to Report Data Breaches

Data breaches are a nightmare to all those involved. The **subjects of the data** are partially or fully exposed, possibly destroying the barrier between their public and private selves, as well as leaving them vulnerable to threats, such as scams, doxing and more. For **companies**, data breaches mean liability, additional costs, legal fees and a potential loss in standing with the consumers of their products and services. Finally, for **governments**, data breaches and leaks may mean grave security risks which could result in catastrophic events, such as the sabotaging of key infrastructure, rigged elections and other events, the likes of which require no Hollywood movie to fathom. In dealing with the potential for such breaches, the LGPD offers a solution, though it lags behind the GDPR, leaving those under its protection wanting.

Both the LGPD and the GDPR stipulate that organisations are required to report data breaches to their local protection agencies or authorities. However, the GDPR soldiers on, stating that such an organisation would have up to 72 (seventy-two) hours to report a data breach[26] – a countdown which commences from the first discovery of the issue. Many tech giants will push this line, preferring to pay a weekly or daily fine and fixing the problem behind closed doors, rather than losing shareholder confidence and, therefore, more money. Though this problem could be fixed by tweaking the available sanctions so as to make them more

[26] Art. 33 GDPR "Notification of a personal data breach to the supervisory authority" Retrieved on the 22nd of July 2020

persuasive, this topic is deficient from the get-go when it comes to the LGPD, which fails to provide a firm deadline for such an act of compliance, choosing instead to revert to the familiar abstract, in its article 48, which reads, "*the controller must communicate to the national authority and to the data subject the occurrence of a security incident that may create risk or relevant damage to the data subjects (...) in a* ***reasonable time period****, as defined by the national authority*"[27]. The national authority in question, the ANPD, is yet to provide a definitive timeframe.

Although the matter of ambiguity can, as previously stated, be a positive force for data subjects, especially in countries such as Brazil, where the judiciary branch is very active and pro-consumer, there are still multiple instances of vagueness in the LGPD which leave much to be desired – on the subject of data breaches, this is apparent.

Fines

The cost of litigating in the United States of America, when compared to Brazil, for instance, is astronomical. In the US, legal fees are higher, court costs are superior, claims are more expensive and class actions are not only a fact of life, but a high-dollar one, at that. Million-dollar settlements have been reached over the loss of a finger in the US[28], whilst a Brazilian who loses an entire arm's function might struggle to attain an indemnity above $40,000[29]. It is either a bizarre fact of life that indemnity comes at such a high cost, in places such as the US, or that it is relatively dirt-cheap, in countries such as Brazil. Regardless, following suit, the LGPD lacks much of the grit found within the GDPR and its international counterparts when it comes to fines and indemnities.

Within the GDPR, fines can require organisations to pay up to €20 million, or 4% of the organisation's annual global revenue, **whichever is highest**[30]. For companies such as Facebook or Google, a 4% annual **global** revenue loss packs a punch. Such a policy gives the GDPR the bite to go along with its bark.

---

[27] "LEI Nº 13.709, DE 14 DE AGOSTO DE 2018", art. 48. Retrieved on the 22nd of July 2020

[28] "$1,400,000 Settlement for Union Carpenter Who Lost Fingertips in Saw Blade Accident" Retrieved on the 22nd of July 2020

[29] "Operário que perdeu braço em siderúrgica tem indenização aumentada para R$ 200 mil" Retrieved on the 22nd of July 2020

[30] "REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL". Archived from the original on 10 November 2017. Retrieved on the 23rd of July 2020

Conversely, the LGPD[31]:

A. Caps the fine to 2% of a private legal entity's revenue.
B. Restricts the fine's calculation to revenue generated in Brazil.
C. Caps the fine further, by stating it may not exceed R$50 million – roughly equal to €7.8 million, at present exchange rates.

Whereas the GDPR states 'X' or 'Y', or '**whichever is highest**', the LGPD states the opposite, in **lower values**, with the addendum of '**whichever is lowest'**. Before the tech giants the LGPD seeks to guard its citizens against, not exclusively, though perhaps primarily, €7.8 million is a drop in the ocean. With a market capitalisation of $741 billion and revenue of $160.74 billion in the most recently reported fiscal year[32], the figure displayed in euros could be paid off by Google ten times over, in the course of a day. As such, the LGPD really needs to change its perspective on fining, if it is to stand a chance at persuading, never mind coercing, big tech into falling in line.

Though the act of calculating fines is extremely arbitrary and, when overly stringent, can lead to economic stagnation and the suppression of innovation, the opposite can lead to a further disparity of arms between data subjects and service providers. Moreover, though the list of variables added to any given calculation can be infinite, there are some points which are vital and should be kept in mind – for this, one turns to the researchers at CTS, or FGV's '*Centro de Tecnologia e Sociedade*'.

Vulnerability of the Data Source

CTS' proposals come from an understanding that the LGPD is, in fact, a necessity. Not only that, the entity understands that the protection of data, whether for reasons of individual freedoms and/or economic impetus, is a matter which touches on legal pillars of the most varied fronts – be those constitutional, civil, penal or other. As such, the suggestions made by the

[31] https://gdpr.eu/gdpr-vs-lgpd/ Retrieved on the 22nd of July 2020
[32] "Google: annual revenue worldwide 2002-2019" Published by J. Clement, Feb 5, 2020. Retrieved on the 23rd of July 2020

researchers in question were founded and proposed with the understanding that, in order for a positive and effective contribution to be made, all aspects of the life, as represented by the law, must be taken into account.

The researchers at CTS recognise that the LGPD is amongst one of the most anticipated laws within the Brazilian legal system, as it deals with matters of data protection in a world where the concern for such is ever-growing. Given this, though the CTS' contributions deal with a multiplicity of issues, as pertains to fines, one must focus on the **vulnerability of the data source**.

When attempting to analyse the LGPD or any of its international counterparts, one must question the reason for the its existence. When defining rules, guidelines, fines and such, it is imperative that the spirit upon which the law is predicated not be corrupted. The 'P' in LGPD stands, after all, for 'protection'. As such, though it would be beneficial to stimulate new and emerging economies, it stands to reason that the law in question was made in order to protects data subjects, whether those be citizens, residents, visitors or others. For this, it must be recognised that there is a huge asymmetry in power, information and resources between those to whom the data belongs vs. those who are manipulating the data in some fashion – hence, the vulnerability of the data source.

In categorising the vulnerability of data sources, CTS has broken the same down into five, main categories, those being:

I. Technical Vulnerability

The holder has no knowledge specifics about the processing of data to which personal information is subject. With the rapid development of new technologies, this gap can often widen, becoming cruelly apparent in communities where formal education on such matters is lacking, As such, this often results in the same relying heavily upon the good faith of others to ensure that his or her rights are not infringed upon.

II. Judicial Vulnerability

Also taken to be understood as a matter intrinsic to technical vulnerability, judicial vulnerability speaks to the difficulties that the subject, from which the data emanates, faces in the fight for the defence of his or her rights, whether administratively or judicially. This could be a result of the lack of access to the proper tools, as well as to the lack of knowledge, as far as how to go about using such tools.

III. Political or Legislative Vulnerability

Political or legislative vulnerability stems from the lack of organization of the data subject, since there are no associations or bodies "capable of decisively influencing in containing harmful legal mechanisms that end up generating real legal monsters"[33]. This, in turn, furthers the asymmetrical nature of the relationship between data subject and service provider.

IV. Psychological or Biological Vulnerability

As is common in today's world, subjects are often bombarded with huge quantities of stimuli which aim to influence their decisions, altering their behaviour in certain ways possibly leading to the detriment of the protection of one's own, personal data. A common tool in marketing, when applied amply and with generalised targets, directed advertising can be intrusive, at the very least. When a citizen's private data is utilised in a 'big brother'[34] fashion, however, that intrusiveness quickly deteriorates into real illegality and the downright abuse of power via inappropriate obtention of information.

V. Economic and Social Vulnerability

Born of the disparities in strength between data processers and data subjects, it becomes self-apparent that there are vulnerabilities to be taken into account when comparing a single citizen, who finds him or herself fighting against a tech giant, such as Google or Facebook. Truly, this David vs. Goliath scenario is the extreme, though it serves to show a defined

---

[33] MORAES, Paulo Valério Dal Pai. Código de Defesa do Consumidor: o Princípio da Vulnerabilidade. 3. ed. Porto Alegre: Livraria do Advogado. 2009.

[34] Term 'Big Brother', retrieved from britannica.com. referring to George Orwell's 1984 depiction of constant surveillance. Retrieved on the 23rd of July 2020

end to the spectrum of asymmetry of power, within which many may already, or will, find themselves. As such, the need for the LGPD to even the forces on the battlefield, quite similarly to the way in which Brazilian Consumer Law goes about its business, is evident.

There is a saying in the UK, that a chain is as strong as it's weakest link. It is true for a bridge, as it is for a society and its accompanying legislation. In analysing the vulnerability of data sources, one is also analysing the weakest links in the equation, and the creation of a safety net should begin by addressing these.

Awareness of the issues surrounding data source vulnerability, as previously explained, are plentiful. As the LGPD breaks into its new shoes, it should seek to address the issues raised herein, for failure could relegate a law of promise into one of minimal scope of applicability and disuse.

Data Localisation

Data localisation, sometimes known as 'data residency' laws, place regulations on the locales in which data regarding a nation's citizen is to be collected, processed and stored[35]. Such applies even – and especially – to cases where data is to be transferred abroad. In such cases, the data in question will only suffer transfer after the requirements set forth by the local data protection laws and agencies have been met. The notion behind data localisation was born of data sovereignty[36], which is predicated on the same grounds and ideals, though which represents a more umbrella term, as opposed to data localisation's more accurate mission statement.

Countless countries have implemented data localisation laws, and hefty fines for those who do not comply with them. Russia, for instance, which has a history of taking its sovereignty quite seriously, has implemented data localisation in an effort to protect its citizens' data – a fact which became a reality with the implementation of Russia's own data protection law, the

[35] "Data Localization Laws: an Emerging Global Trend". Jurist. Archived version from January 6, 2017. Retrieved on the 23rd of July 2020

[36] Irion, Kristina (2012-12-01). "Government Cloud Computing and National Data Sovereignty". Policy & Internet. 4 (3–4): 40–71. doi:10.1002/poi3.10. ISSN 1944-2866.

'*Federal Law of the Russian Federation 'On Personal Data*'[37]. In similar suit, the USA has had unofficial data localisation for quite some time, though it has been common knowledge that, since the Patriot Act[38], passed in the aftermath of 9/11, the defence of data in the country faced a much heightened level of protection. Brazil, though having not undergone a catalyst-like event, could very well implement data localisation laws, which it has not yet to date.

When it comes to why countries should apply data localisation, the reasons are multiple. On a macro scale, the issue of protecting citizens and their data is very real. By storing the information in question within the territory of the country, it becomes, invariably, much easier to protect the same. Furthermore, the process of requesting that data be stored, altered or deleted becomes a lot more expedient, given that one can petition one's own government, without having to navigate international laws and/or engage foreign judiciary branches and agencies. Moreover, when it comes to the matter of taxation, one could very well say the same.

Data has suffered a comparison to oil on multiple occasions and not just in this paper. In order to effectively tax the same, such can best be done via strict geographical and migratory controls. In treating data like any other resource, one could see the benefits and ease with which the same might be taxed, should this take place before the data leaves the country. Large server room and data centres could effectively provide this safe location, ensuring Brazilian data is being received on the nation's terms and not the inverse. Likewise, one could definitely see stratified data localisation being a reality in the future – meaning data localisation on state and municipal levels.

If one recalls the discovery of oil off the coast of Rio, at the start of the previous decade, and the commotion which followed, one can draw comparisons between the same. The governor, at the time, cried at the loss of the revenue to the state[39] - albeit for conflicting reasons, though he cried, nonetheless. This was due to the fact that the federal government had announced that, despite the oil having been found off the coast of a specific state, in this case, Rio de Janeiro, the revenue from its extraction would be used to benefit all states within the federal union, as opposed to only Rio. With data presently being the most precious commodity in the world, it would come as no shock if states made a push to have state-side data

[37] Arievich, Pavel (1 June 2012). "Data protection in Russian Federation: Overview". Practical Law Company.
[38] "Bill Summary & Status 107th Congress (2001–2002) H.R.3162 Major Congressional Actions", Retrieved on the 23rd of July 2020
[39] "Cabral chora e diz que emenda Ibsen quebrará Estado do Rio" Retrieved on the 23rd of July 2020

localisation, on top of that of the federal level, in order to create additional protections for its citizens, as well as to further tax the data, in question.

Despite the fiscal repercussions which come with data localisation, the need for the same cannot be understated. Factually, if Brazil does not make money off the data emanating from its citizens, other countries and companies will. Thus, making this untapped market produce for Brazil could and should be a priority. Again, the importance of safely securing one's citizenry and their data should not be minimised. Such is why it came with sad tidings when the LGPD arrived without proper provisions to ensure that data localisation would be a reality. Still, on the 29th of September 2020, a bill was proposed in congress, seeking to correct this error. Bill 4723/2020[40] looks to impose data localisation requirements within Brazil, prohibit the use of cloud computing for extraterritorial processing of data, as well adding a few more hoops to be jumped through for those joining the Brazilian ANPD.

[40] "Brazil: Bill on data localisation and appointment of ANPD members introduced into Chamber" Retrieved on the 23rd of July 2020

Conclusion:

Now, one must forgive the creative and academic liberties taken within this chapter, as it might lead some to believe one's analysis of the LGPD to be overly critical or negative. Instead, one has taken the initiative to define this concluding chapter, as one which possesses some remedies – especially as relates to the more troublesome aspects of the LGPD, as discussed in previous sections of this paper.

The LGPD is not a perfect piece of legislation, though it very much stands to be a step in an excellent direction. In some ways, it falls behind the GDPR, though in many others it supersedes it. Commencing with the boons of the LGPD, one should mention personal data, the manner in which it is classified and how issues surrounding it are enforced.

The LGPD's classifications of data into personal, personally identifiable and sensitive is a great achievement, in that the first is not lacking in protection. Instead, additional protections are conferred, based on the sensitivity of the data subject and the data itself. This progression of heightening defences serves its just purpose – ensuring that the LGPD follows through with its originally intended objective, which is to protect data and data subjects.

On the matter of data subject rights, the LGPD goes as far as to almost carbon copy the GDPR. Whilst, academically, the practice might seem cheap and unoriginal, legally, this is a grand move. This, as it allows for easier compliance between the EU and Brazil, whilst not sacrificing the protection of the data subjects – given that the right afforded to the same, by the GDPR, are actually quite ironclad. In other words, the manner in which data subject rights are handled by the LGPD leave little to be desired, having found a good balance between easing of compliance practices for businesses and strengthened protection for data subjects.

When contemplating extraterritoriality as a factor of data protection, it goes without saying that, in the globalised world of today, a law which aims to govern data across international borders cannot be relegated to enactment and consequent enforcement solely on a national level. It must, instead, aim to defend all data subjects worthy of its protection, regardless of physical borders. Given this, the LGPD continues to impress, having extraterritoriality in a fashion which allows for a more ample protection of data subjects under its purview, as well as generating better standards and practices for foreign companies seeking to be in compliance.

Nonetheless, the LGPD is not without fault and failure. Despite the law being a new mark for individual protections, it still lacks some serious addendums, without which large deficits in enforceability become glaringly apparent – the most notable of which comes in the form of legal omissions, which in turn result in inefficiencies, as well as dependencies on subsidiary laws not crafted specifically for the purpose of the protection of data and its subjects.

In the case of Data Protection Officers, the trouble emanates from lack of legislative clarity, as well as from the ability to outsource the same to third parties and non-natural persons. Thus, when definitive rules are not established, attributing **extensive responsibilities** to DPOs, one is left with the generalisations found within the legal text. These are reductive and lacking in any real substance – not to mention possessing of a frightening lack of clarity as to the qualitative nature of candidates to such positions. Furthermore, the central idea behind DPOs comes in the form of enforcement of the LGPD, as well as in the compliance of companies with the same. The spirit of the idea is to hold those collecting, processing and storing information liable for their actions, should they breach the LGPD. Consequently, allowing for this position to be outsourced and, therefore shifting and mitigating risks intended to alter a company's behaviour towards data, ends in a simple addition of costs for said company – a fact which could translate to additional externalities, paid for and by the data subjects.

On the subject of data breaches, the LGPD's ambiguity as to the timeframe in which such must be reported is a travesty. When using terms such as 'reasonable', in reference to the time one must take to act upon a breach, one generates some heavy externalities. The first comes in the form of lack of protection, felt mostly by data subjects. The second comes in the form of legal uncertainty, as companies have no idea as to whether their pace is hasty and careless or lethargic and irresponsible. As usual, these legal vacuums generate an additional burden upon the judiciary, which will, as usual, be forced to fine-tune expectations vs. reality, only later to be accused of judicial activism.

On the other hand, perhaps one of the simplest problems, requiring the meekest of remedies, is the vector by which the LGPD approaches fines, which currently feel somewhat redundant. Fines have multiple purposes, though two main drives are deterrence and reparation – neither of which can be realistically established via the amounts required as payment for breaching the LGPD. Brazil has a huge stake in the internet and the usage of the same, within the country, reflects that. Given this, one would staunchly argue that the caps on fines could drastically be increased without a single tech giant feeling the need to pull out of Brazil.

Furthermore, there is no logical reason for restricting the calculation of fines to operations within the confines of the national borders, given that the LGPD had extraterritorial application, as well as after seeing how much more successful the GDPR's lack of such a restriction can be.

The most complex issue the LGPD might have to deal with is the vulnerability of data sources. Given that Brazil has many demographic discrepancies, the lack of this uniformity within the population tends to translate socially. There is a huge gap between those with access to technology and those without. The same can be said for access to education, the judiciary and more. In order to tend to that asymmetry of power and information, the researchers at CTS made a compelling argument for the implementation of the '*Theory of Dialogue Between Sources*'[41]. In this theory, the multiplicity of laws which suffer contact with the LGPD would serve to create reciprocal fortification, as opposed to furthering much of the ambiguity seen in some legal texts.

Given the immense amount of overlap which will, naturally, occur between these different sets of laws, norms and regulations, the need for **harmony** between the same becomes instantly apparent. The fortifying of the individual through this harmony is well exemplified by the CDC, or the Brazilian Consumer Defence Code, which works in unison with the Civil Code to produce results. In dealing with a party that finds itself at a significant disadvantage, when it comes to lack of information, know-how, technical or monetary capacity, it is evident that the LGPD requires many of the guarantees offered to consumers by the CDC, in order to even the playing field. Much to CTS' satisfaction, one can be sure, the judiciary has already discussed and seems to favour the application of this '*Theory of Dialogue Between Sources*' in scenarios involving the LGPD and other norms with which such might endure some lasting conflict.

In a conference between the judiciary and promoters of legal doctrine, a professor at the Federal University of Rio Grande do Sul (UFRGS), Cláudia Lima Marques, made a prominent comment on the issue, stating that, when it comes to the LGPD, "*This is a revolutionary cross-*

[41] In recognising that the Brazilian data protection law deals with numerous other laws, norms and regulations, the concern then becomes how to make these compatible with one another, ensuring they complement each other, as opposed to weakening the purported texts.

cutting law. All the others will adapt. [The Theory of] Dialogue from Sources is needed to avoid injustice"[42].

Just as it is needed, this theory will most likely suffer heavy application in the years to come. Given the propensity for the Brazilian judiciary to be pro-consumer, as well as Brazil's staggering 151.1 million internet users (projected to be 169 million users by 2023)[43], the country should not and cannot afford to have its most prominent data protection law roadblocked between competing legislations, as such would accrue tremendous deficits – both financially and in the realm of personal, individual freedoms and protections.

Finally, despite all its flaws, a disclaimer must be made – Brazil would be lost without the LGPD. Had the LGPD not been adopted, many of the data protection issues the country faces would be regulated by the Brazilian Civil Rights Framework for the Internet, known in Brazil as the '*Marco Civil da Internet*'[44]. Though this framework was quite a necessary addition when passed, it lacked the complexity necessary of a true and fleshed out data protection law – most especially during a time in which technological advances and the risks to personal privacy have spiked like never before. Additionally, whilst it granted some key protections through its policies on data governance, it also stripped others away[45] and suffered occasional bouts of authoritarian use[46].

Thus, despite all criticism, one can definitively state that the LGPD is a force for good within Brazil. Moreover, though it seems to lag behind the GDPR in many of its practical aspects, the compliance needs required of the LGPD make for easier ventures between those subject to the GDPR and the LGPD. Yet, legislators and advocates for civil liberties and data protection must not rest upon their laurels. With the speed in which technology evolves, any legislation passed will always find itself, necessarily, behind. If the LGPD is a GDPR Lite, then every effort must be made to equalise protections, or even, to lead the charge.

---

[42] "Seminário no STJ discute implementação da Lei Geral de Proteção de Dados" Retrieved on the 24th of July 2020

[43] "Brazil: number of internet users 2015-2025." Published by José Gabriel Navarro, Jul 20, 2020 Retrieved on the 24th of July 2020

[44] "The Brazilian Civil Rights Framework for the Internet". FGV Direito Rio. May 9, 2014. Retrieved on the 24th of July 2020

[45] "Brazil Squanders Chance At Geopolitical Influence". 2012. Retrieved August 12, 2016.

[46] "São Paulo Court of Justice - Justiça determina bloqueio do aplicativo WhatsApp" Archived 2015-12-20 at the Wayback Machine, Comunicação Social TJSP, São Paulo Court of Justice, Retrieved on the 24th of July 2020

Bibliography

Laws, Treaties, Regulations & General Legislations:

The Brazilian General Data Protection Law (LGPD) – Unofficial English Version" Retrieved on the 20th of July 2020.

EUR-Lex – 32016R0679 – EN – EUR-Lex. eur-lex.europa.eu. Archived from the original on 17 March 2018. Retrieved on the 20th of July 2020.

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, LGPD. Retrieved on the 20th of July 2020.

Universal Declaration of Human Rights. United Nations. Retrieved on the 21st July 2020.

PEC 17/2019" Retrieved on the 21st of July 2020

European Parliament and Council of European Union (2016) Regulation (EU) 2016/679. Retrieved on the 21st of July 2020

LEI Nº 13.709, DE 14 DE AGOSTO DE 2018, art. 11. Retrieved on the 21st of July 2020.

LEI Nº 8.069, DE 13 DE JULHO DE 1990 Retrieved on the 21st of July 2020

Art. 33 GDPR "Notification of a personal data breach to the supervisory authority" Retrieved on the 22nd of July 2020

"Bill Summary & Status 107th Congress (2001–2002) H.R.3162 Major Congressional Actions", Retrieved on the 23rd of July 2020

"The Brazilian Civil Rights Framework for the Internet". FGV Direito Rio. May 9, 2014. Retrieved on the 24th of July 2020

Miscellaneous & Media:

Christopher Hitchens , "Christopher Hitchens: Empowerment of Women". YouTube. Retrieved on the 21st of July 2020

Term 'Big Brother', retrieved from britannica.com. referring to George Orwell's 1984 depiction of constant surveillance. Retrieved on the 23rd of July 2020

Academic Articles:

“Contribuição do Centro de Tecnologia e Sociedade da FGV DIREITO RIO ao debate público sobre o Anteprojeto de Lei de Proteção de Dados Pessoais” CTS, FGV Direito Rio. Retrieved on the 20th of July 2020.

"Estonia", Freedom on the Net 2013, Freedom House, 2013. Full Report Available here. Retrieved on the 21st of July 2020

"Estonia, where being wired is a human right", Colin Woodard, Christian Science Monitor, Retrieved on the 21st of July 2020

"Data Localization Laws: an Emerging Global Trend". Jurist. Archived version from January 6, 2017. Retrieved on the 23rd of July 2020

Irion, Kristina (2012-12-01). "Government Cloud Computing and National Data Sovereignty". Policy & Internet. 4 (3–4): 40–71. doi:10.1002/poi3.10. ISSN 1944-2866.

Arievich, Pavel (1 June 2012). "Data protection in Russian Federation: Overview". Practical Law Company.

Books and other Publications:

DeFoe, Daniel (1726). The Political History of the Devil, As Well Ancient as Modern: In Two Parts. London: Black Boy in Pater-noster Row. Online version available here.

MORAES, Paulo Valério Dal Pai. Código de Defesa do Consumidor: o Princípio da Vulnerabilidade. 3. ed. Porto Alegre: Livraria do Advogado. 2009.

Lorge, Peter A. (2008), The Asian Military Revolution: from Gunpowder to the Bomb, Cambridge University Press, ISBN 978-0-521-60954-8

Tunis, Edwin (2002). Wheels: A Pictorial History.

News Articles:

"People Are Becoming More Reluctant To Share Personal Data, Survey Reveals" Forbes. Retrieved on the 21st of July 2020.

"Finally, the world is getting concerned about data privacy." Retrieved on the 21st of July 2020.

"Digital 2020: Brazil". DataReportal – Global Digital Insights. Retrieved on the 21st of July 2020

"Esports in Brazil: Key Facts, Figures, and Faces" Retrieved on the 21st of July 2020

Wyatt, Edward (April 8, 2011). "House Votes Against 'Net Neutrality". The New York Times. Retrieved 21st of July 2020

"10 Countries with GDPR-like Data Privacy Laws" Retrieved on the 21st of July 2020

"Uber chega ao Brasil e não quer polêmica". 27/05/2014 27th of May 2014. Retrieved on the 21st of July 2020

"What is the LGPD? Brazil's version of the GDPR" Retrieved on the 22nd of July 2020

"$1,400,000 Settlement for Union Carpenter Who Lost Fingertips in Saw Blade Accident" Retrieved on the 22nd of July 2020

"Operário que perdeu braço em siderúrgica tem indenização aumentada para R$ 200 mil" Retrieved on the 22nd of July 2020

"Google: annual revenue worldwide 2002-2019" Published by J. Clement, Feb 5, 2020. Retrieved on the 23rd of July 2020

"Cabral chora e diz que emenda Ibsen quebrará Estado do Rio" Retrieved on the 23rd of July 2020

"Brazil: Bill on data localisation and appointment of ANPD members introduced into Chamber" Retrieved on the 23rd of July 2020

"Seminário no STJ discute implementação da Lei Geral de Proteção de Dados" Retrieved on the 24th of July 2020

“Brazil: number of internet users 2015-2025.” Published by José Gabriel Navarro, Jul 20, 2020 Retrieved on the 24th of July 2020

"Brazil Squanders Chance At Geopolitical Influence". 2012. Retrieved August 12, 2016.

"São Paulo Court of Justice - Justiça determina bloqueio do aplicativo WhatsApp" Archived 2015-12-20 at the Wayback Machine, Comunicação Social TJSP, São Paulo Court of Justice, Retrieved on the 24th of July 2020

“Elon Musk says there's a chance his AI-brain-chip company will be putting implants in humans within a year.” Retrieved on the 21st of July 2020.