CATÓLICA
FACULDADE DE DIREITO
ESCOLA DE LISBOA

CATÓLICA
Global
School of
Law

BRAZILIAN GENERAL DATA PROTECTION ACT

CONSOLIDATION OF A GLOBAL PRIVACY PROTECTION STANDARD

Estêvão Nascimento Orcini
Master of Transnational Law Dissertation
Under the orientation of Prof. Dr. Pedro Maia Garcia Marques

Lisbon,
June 2020

CATÓLICA
FACULDADE DE DIREITO
ESCOLA DE LISBOA

CATÓLICA
Global
School of
Law

BRAZILIAN GENERAL DATA PROTECTION ACT

CONSOLIDATION OF A GLOBAL PRIVACY PROTECTION STANDARD

Estêvão Nascimento Orcini

Master of Transnational Law Dissertation

Under the orientation of Prof. Dr. Pedro Maia Garcia Marques

Lisbon,
June 2020

ACKNOWLEDGEMENTS

To Professor Pedro Garcia for his precious insights, availability and cordiality.

To Beatriz Moreira for all her affection, especially while this thesis was written down.

To Nuno Morgado for the roof, wine and such delightful friendship.

To Felipe Assis for helping me access the main online bases of articles without being reached by any spyware.

To Maurício Queiroz, Joel Orcini and Teresa Orcini, for being around if it was necessary.

To myself, since today I am the one who has less time and money after all.

BRAZILIAN GENERAL DATA PROTECTION ACT

Consolidation of a global privacy protection standard

Abstract: Since the European Union has enacted the Regulation No. 679/2016, the GDPR, the debate over data protection have been acquiring enormous relevance and is currently on the global agenda from east to west. The compilation of individuals' information is far from being new and it has been practiced for some decades, even for-profit purposes. The GDPR is not the first law framework committed to look after data protection either. Yet it seems that only in the last five years the debate reached other states than the ones hosting the giant tech companies' headquarters, like US and a few European countries, and a new era has been emerging for personal data protection. Besides, the discussion nowadays developed beyond the privacy and transparency debate, being rather focused on deeper issues, such as the maintenance flow of innovation and the not so hard to imagine ending of the liberal democracy at least as we know it today. To deal with this new panorama, many governments are creating or amending their country regulations. Among the ten wealthiest economies worldwide, only China have not published a binding data protection draft bill, at the same time as Brazil is the last country to regulate data protection by means of a single comprehensive. Supposed to be enacted alongside with the Brazilian Civil Framework of the Internet in 2014, Brazil postponed its General Data Protection Act up till August 14th, 2018, when Law No. 13.709/2018 was finally approved. This new law, which will come into effect on August 2020, already represents a radical change in the way such matter is treated in Brazil, yet, on a first glance, it seems it does not innovate much and gives a sign of consolidation of what has been considered the global privacy protection standards. The purpose of this paper is to verify whether and to what degree the Brazilian General Data Protection Act follows the matrix of the main lawmakers worldwide, those who have influence power, namely, the GDPR, current considered the most relevant personal data protection law in force, and the US correlated law. This analysis will be conducted through a closer look to the main concepts and values that permeate the most relevant discussions and by performing comparison between the main aspects considered in both the EU and US approach, to finally dwell on the most important points of the Brazilian law.

Key Words: data privacy, transnational data protection, GDPR, LGPD

List of Abbreviations and Acronyms

CCPA	Californian Consumer Protection Act
EU	European Union
GDPR	EU General Data Protection Regulation
LGPD	Brazilian Data General Protection Act
STJ	Brazilian Superior Court of Justice
US	United States

SUMARY

Acknowledgments……..ii
Abstract……..iii
List of Abbreviations and Acronyms.....…….....iv

INTRODUCTION……..1

Chapter I – PERSONAL DATA PROTECTION: RIGHT TO WHAT?.....3
1.1. The age of surveillance……..4
1.2. Protecting Privacy……..6
1.3. The benefits granted in return for privacy violation……..8
1.4. Privacy as fundamental right, not commodity…….....10

Chapter II – IS THERE A GLOBAL DATA PRIVACY STANDARD ON THE WAY?.....13
2.1. The EU and US historical approach to data privacy……14
2.2. Unilateral regulatory globalization - Brussels and California effect……..16
2.3. GDPR versus CCPA……....18
2.3.1. GDPR overview……...19
2.3.2. CCPA overview……...21
2.3.3. Divergences and Convergences……...22
2.4. Do we have a winner in the global trend running?.....24

Chapter III – THE BRAZILIAN GENERAL DATA PROTECTION ACT……27
3.1. The ten principles to follow……28
3.2. Individual's rights and processing agent's obligations under the LGPD…….29
3.3. Other relevant aspects: extraterritorial scope, cross-border data transfer and enforcement……32
3.4. Consolidation of a standard law?.....34

CONCLUSION…….....38

Bibliography……..39

INTRODUCTION

Talking on how the global economy is undergoing a digital transformation at full tilt speed is becoming commonplace. Yet, as any disruptive movement, the growth and evolution of the digital economy, the activity that results from billions of everyday online connections among people, businesses and devices, inevitably raise important challenges among which is privacy protection. In this new digital market model, technologies have delivered innovation and consumer welfare mostly in exchange for more information. Such technologies that have transformed our habits, making us more connected, have also improved the apprehension of our personal data, created even more detailed records our daily live and used this to profit from them. This large scale use of data is transforming business models, products, services and social interactions.

Finding one not impressed by the convenience of contracting products and services through internet is a hard work. Either "this is worth it" or "I 've got nothing to hide" statements used to be people's reply to the privacy menace. The exchange of such data for security and convenience that seemed fair and has been working well in the recent past, however, gradually becomes controversial. Interests then concerning how far these companies could go in exploiting data without disclosing any further information have only recently stopped being dealt with punctually to become a common issue among scholars and governments.

At the forefront of data protection, the European Union enacted the General Data Protection Regulation (GDPR), which is committed to provide a single set of rules for all EU member states, directly applicable under EU law, which took effect on May 25, 2018. One month later, California enacted the California Consumer Privacy Act (CCPA), which entered into force on January 1st, 2020, emerging as a national model and inspiring other US states to adopt similar measures. On July 27th, 2018, India published a draft bill for a new, comprehensive data protection law and, only a few weeks after, on August 14, 2018, Brazil approved its data protection act. Except for China, thus, the most relevant economies in the world have data privacy and protection on the agenda.

Throughout this paper our aim will be: because of the capacity of the EU to irradiate its data protection legislation and consolidate it as a global privacy protection standard, the Brazilian General Data Protection Act (LGPD[1]) has the GDPR as its main inspiration. AAs plenty other territories also done. Our argument thus proceeds in three steps. During the first

[1] Its anachronism for Portuguese – *Lei Geral de Proteção de Dados.*

chapter, we go through crucial concepts to understand data protection, such as surveillance and privacy. In the second chapter we extend our analysis to the two jurisdictions that are powerful enough to influence domestic regulations outside their borders, European Union and US. Attention will be drawn to their historical approach to data privacy and providing an overview over their leading regulation, the GDPR and the CCPA, respectively. Finally, on our third chapter we address the main features of the LGPD, among which, the principles it is based on, individual's rights and processing agent's obligations, in order to compare it, the GDPR and the CCPA, and just before we present our conclusions.

CHAPTER I - PERSONAL DATA PROTECTION: RIGHT TO WHAT?

Over the last 20 years, technological development brought a significant change in the methods, material, or equipment used to accomplish a task. It is constantly transforming our habits, apart from improving the apprehension of our personal data and creating more detailed records on us. The exchange of such data for security and convenience that seemed fair and have been working well in the recent past thus has come to be questioned. A survey conducted on June 2019 in US shows that more than 80% of public consider the potential risks they face because of data collection outweigh the benefits[2]. The academic warning that an architectural change in the means data is collected, analyzed and applied is on the way as Big Data is upon us (meaning an increase in volume collection, analysis velocity and questions about the veracity of the inferences made).[3]

For different reasons, people are talking greatly about data protection worldwide. Europe has enacted its data protection law the GDPR, which was very well received (yet some critical voices argued that it brought insufficient protection against big data inferences[4]). The adoption of a data protection legislation is also part of the emergent countries' agenda, aiming to ensure an adequate level of guarantees in accordance with EU patterns. In its turn, US reveals a collective sense that data security has become less secure[5].

But less secure how? What does such laws are really concerned to protect? The usual and most obvious answer is privacy. But even privacy is a complex and misunderstood concept as we will see. Many scholars are thinking, researching and writing about it, but the whole picture is still difficult to paint. In this chapter we will look closer to the privacy concept and why we are, or should be, pursuing to protect it from both state and private surveillance despite all the benefits they apparently offer in return for personal data. Without being able to understand it, we would not be ready to discuss data protection laws that comes next.

---

[2] Brooke Auxier *et al.* (2019, November 15), Pew Research Center, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*. Available at https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.

[3] Zarsky, Tal, *Incompatible: The GDPR in the Age of Big Data*. Seton Hall Law Review, Vol. 47, No. 4(2), 2017, at 998-999. Available at: https://ssrn.com/abstract=3022646.

[4] See, *e.g*., Zarsky, supra note 2; and Wachter, Sandra and Mittelstadt, Brent and Floridi, Luciano, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*. International Data Privacy Law, 2017. Available at: https://ssrn.com/abstract=2903469.

[5] According to more than 70% of adult opinions. Auxier, supra note 2.

1.1. The age of surveillance

Surveillance had been relegated to totalitarian states throughout history as it was thought a unique feature of their *modus operandi* [6]. Yet such autocracies were discovered not being alone when it came to looking more closely. Democratically elected governments has shown a keen willingness in surveillance of the public as a measure of counterterrorism, intellectual property protection, among other concerns[7]. In the most outrageous event that came public in last years, the National Security Agency (NSA), a US body responsible for government cybersecurity, was found recording calls of millions of Americans for years without their consent or even knowledge in the name of state security[8].

In the opinion of leading scholars, we are all living in an age of surveillance even we do not realize it[9]. The digital technologies that have revolutionized our routine over the past decades are also able to reach people anywhere. More than that, such fast innovations have also created increasingly detailed records about our daily lives and the entities that want to surveil ever more multiplied together with the technologies of surveillance[10]. Companies thus have also become interested in data, inaugurating a new era that Shoshana Zuboff called "surveillance capitalism[11]".

David Lyon defines surveillance as "the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction"[12]. Whether performed by government agencies or private parties, the interests lie not only in collecting and recording details of personal information, but also in organizing them to provide ground for action toward the people concerned[13]. As the concept suggests, surveillance does not necessarily encompass harmful intent; it is a natural and basic social process. What has changed in the last hundred years to turn on our warning signal is the rise of mass surveillance, which ranges from the benign to the repressive and fuels universal pressures on privacy[14].

---

[6] Richards, Neil M., *The Dangers of Surveillance*. Harvard Law Review, 2013, at 1934. Available at SSRN: https://ssrn.com/abstract=2239412.
[7] *Id.*, at 1937.
[8] In 2013, together with The Guardian's journalists, Edward Snowden disclosed the NSA secret program on mass surveillance. See more at https://www.theguardian.com/us-news/the-nsa-files.
[9] See, e.g., Neil, supra note 6; and Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs, 2019.
[10] Neil, supra note 6, at 1936.
[11] Zuboof, supra note 9.
[12] Neil, supra note 6, at 1937.
[13] Rule, James B., *Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience.* Oxford University Press, 2012, at. 14.
[14] *Id.*

States, whether totalitarian or not, remain attracted to save as much information as they are able to absorb, for many reasons, from better mapping people's needs, to the most hideous interests, such as when trying to control political bias by handling available information. In its turn, companies wish to track individuals behavior and use as free raw material for very well-known or still hidden commercial practices[15]. Conscious of the consequences of such process, John Naughton warns us that:

> [t]he combination of state surveillance and its capitalist counterpart means that digital technology is separating the citizens in all societies into two groups: the watchers (…) and the watched[16]

Which means profound consequences for democracy as such asymmetry of knowledge is translated into asymmetries of power considering that most democratic societies have at least some degree of oversight of state surveillance while "we currently have almost no regulatory oversight of its privatized counterpart[17]". We are already aware that human experiences have been translated into data by online enterprises. Yet, while some of these information are applied to service improvement as we like to think, the most part is declared as proprietary *behavioural surplus to be* used for creating tradeable *prediction products* through machine intelligence processes[18]. This is what Zubboff called surveillance capitalism the current pattern on which we have little control.

Companies activities concerning the data collection have been on the European agenda for years[19] and more recently has become part of discussions around the world due to the GDPR success in spreading its ideas (see Chapter 2 and 3). Some regulatory rules and tools have been provided to limit the process of personal data online, as the adequacy rule that limits a transfer of personal data to a third country or to an international organization which does not ensure an adequate level of protection[20]. But it is not difficult to realize it is not enough. The civil society still fails to completely understand why surveillance is harmful, whilst it is trapped in an

[15] Zuboof, supra note 9, introduction.
[16] Naughton, John, *The goal is to automate us': welcome to the age of surveillance capitalism.* Available at:https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook
[17] *Id.*
[18] Naughton, supra note 16, at 8.
[19] EU has been regulating it closely at least since its 1995 Data Protection Directive.
[20] General Data Protection Regulation 2016/679, Article 45.

involuntary merger of personal necessity and economic extraction[21]. The answer has everything to do with privacy, how it is far from being well articulated and thus "we frequently lack a compelling account of what is at stake when privacy is threatened and what precisely the law must do to solve these problems[22]."

1.2. Protecting Privacy

Privacy issues did not arise from the twenty-first century debate. Controversies over privacy reflect long-running ethical and political tensions between individual prerogatives and claims of social improvements, since long before the rise of most technologies currently menacing privacy value [23]. Yet, despite of being recognized as a fundamental human right by the 1948 United Nations Universal Declaration of Human Rights and protected by a wide range of countries, either through a direct mention in their constitutional law or the recognition as an implicit constitutional right[24], privacy remained eclipsed until 1960s[25]. The expanding of the telecommunication networks and rising of the organizations developments in finding new ways of capturing data thus have received steadily increasing attention and injected a sense of urgency to these unresolved tensions.

The good news is, since then, many renewed scholars have been researching privacy issues to understand privacy properly[26]. The bad news, in turn, is that privacy remains unclear to most people, including legislators, as a complex value engorged with various and distinct

[21]Soshana Zuboof in an interview for The Guardian. Available at: https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook.

[22] Solove, Daniel J., *Understanding Privacy*. Harvard University Press, 2008, at 2.

[23] Rule, supra note 13, at 10.

[24] Solove, supra note 22, at 3.

[25] In Katz v. United States (1967), the Supreme Court ruled that the government's use of an electronic device to record conversations inside a telephone booth without a warrant violated individual's privacy. Such position was resulted by the weight courts started to give to new technologies as, by the early 1960s, the use of phones grew from 4% to around 80%. Price, W. Michael. *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine.* JOURNAL OF NATIONAL SECURITY LAW & POLICY. Vol. 8, at 11. Available at https://www.law.nyu.edu/sites/default/files/upload_documents/Price%20Rethinking-Privacy-Fourth-Amendement-Papers_2.pdf.

[26] See, e.g., Cohen, Julie E., *Examined Lives: Informational Privacy and the Subject as Object*. Georgetown Law Faculty Publications and Other Works. 810. Available at https://scholarship.law.georgetown.edu/facpub/810; Hartzog, Woodrow and Richards, Neil M., *Privacy's Constitutional Moment and the Limits of Data Protection*. 61 Boston College Law Review (Forthcoming 2020). Available at SSRN: https://ssrn.com/abstract=3441502; and Richards, Neil M. and Solove, Daniel J., *Privacy's Other Path: Recovering the Law of Confidentiality*. Georgetown Law Journal, Vol. 96, p. 123, 2007; GWU Law School Public Law Research Paper No. 249; Washington U. School of Law Working Paper No. 07-03-02. Available at SSRN: https://ssrn.com/abstract=969495.

meanings. Meanwhile the rights commonly opposed to it, as security and innovation, are often much more easily articulated[27]. Hence, the concept of privacy is still considered far too vague to guide lawmaking[28], being an easy target to opposing companies and their spokespersons, strongly interested in associating it to an anti-progressive image, capable of disturbing the cutting-edge imperatives of national security and entrepreneurship[29].

From intimacy and individuality to creativity, freedom of thought and even democracy, all these principles would rest on the privacy protection[30], depending solely on the context. In the context we have been discussing, privacy means the rules governing the collection, use, and disclosure of information[31]. It provides the isolation necessary for contemplation and, as consequence, for the exercise of our cognitive freedom, which, in its turn, enables us to think for ourselves, free to assemble our thoughts and form our own ideals[32]. As noted by Timothy Macklem, privacy makes "possible for people to reach different conclusions and thereby develop different ways of life, the ways of life that liberal societies draw upon for the diversity that makes freedom valuable there[33]". Hence, privacy is essential to democratic governments.

Commenting on privacy, Julie Cohen claim that, more than to be basic for democracy, privacy is also relevant to mold the practice of citizenship. According to her, mostly of our currently experiences have been mediated by search engines and social networking platforms which we daily feed with personal data in the networked society[34]. Such tools cross all the available information to filter and tailor content we will be exposed prioritizing results in ways that reflect their own interests and, of course, advertising money. It means that they select most of what we will watch or read on internet, shaping our comprehension of the surrounding world[35]. Hence, our capacity for democratic self-government and freedom of thoughts is highly dependent on what those technologies make available and it directly impacts on our political culture without prior consultation[36].

---

[27] Solove, supra note 22, at 2.
[28] *Id.*
[29] Cohen, Julie E., *What Privacy Is For*. Harvard Law Review, Vol. 126, 2013, at 1. Available at SSRN: https://ssrn.com/abstract=2175406.
[30] Solove, supra note 22, at 7.
[31] Richards, Neil M. and Hartzog, Woodrow, *Taking Trust Seriously in Privacy Law*. Stanford Technology Law Review 431 (2016), at 434. Available at SSRN: https://ssrn.com/abstract=2655719.
[32] Richards, Neil M., *Intellectual Privacy*. Texas Law Review, Vol. 87, 2008, at 416. Available at SSRN: https://ssrn.com/abstract=1108268
[33] *Id.*, at 416.
[34] Cohen, supra note 23, at 8.
[35] *Id., at 9.*
[36] *Id.*

On Cohen views, privacy is built to protect "situated practices of boundary management through which the capacity for self-determination develops[37]", enabling individuals "to develop critical perspective on the world around them[38]". The permission for the ascendancy of surveillance infrastructures, in this context means the gradually replacement of the liberal democracy as we have conceived it today by what Cohen calls a modulated democracy. Indeed, citizens shall increasingly lack the capacity to form and pursue meaningful agendas for human prosperity due to the pervasively distributed surveillance and modulation by powerful commercial and political interest[39].

1.3. The benefits granted in return for privacy violation

Finding one not amazed by products and services offered by the most technological internet companies is a hard work. After all, who could object the convenience of asking any kind of food just using a smartphone and receiving it after 30 minutes at home? How about going to jog and listening your favorite songs and having the opportunity to share these moments with our friends just posting it at the social medias? Take a photo, swipe through the filters to find the perfect one and hit publish. Not to mention grocery, pharmacy and clothes shopping without leaving home in pandemic times. All of this at the expense of the disclosure of some private information.

"This is worth it" and "I 've got nothing to hide" statements are listened everywhere. People believe that "there is no threat to privacy unless the government uncovers unlawful activity, in which case a person has no legitimate justification to claim that it remain private[40]", as points Daniel Solove. Government programs on gathering of data are usually thought as very limited disclosure of only few particular information to few government officials, being not able to threat personal data protection. With the premise assumption that privacy is about hiding immoral or criminal things, it is common sense thus that only those who are engaged in illegal

[37] *Id.*, at 2.
[38] *Id.*, at 3.
[39] *Id.*, at 7.
[40] Solove, Daniel J., *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*. San Diego Law Review, Vol. 44, p. 745, 2007. GWU Law School Public Law Research Paper No. 289, at 747. Available at SSRN: https://ssrn.com/abstract=998565

activities should be worried to keep information private. Moreover, people also consider security as it was a much higher interest than whatever "minimal" privacy concerns.[41]

. What ,most people do not realize is that the threaten to privacy is daily build by a series of relatively minor acts rather than by flagrant ones[42], with long term consequences so well described by Cohen[43]. Unless it becomes harms to their personal accounts, the issue thus is largely an academic one which is safely ignored.

These ways of justifying programs like data mining or state surveillance – either by denying the existence of a problem, as in the "nothing to hide" argument, or acknowledging it but contending that the benefits outweigh the privacy harms[44] - expressly reveal that people are acting like data factories on internet, providing raw material while ceasing privacy, without being able to notice it. Surveillance can create ultimately chilling effects on essential rights for democracy, harming society while they reduce the range of viewpoints expressed and the degree of freedom with which to engage in political activity. Yet the chilling effects are often very hard to be concretely demonstrated, since the value of protecting against it is not measured simply by focusing on the particular individuals[45].

Surveys show a seemingly trend in which people has started to understand the role their data play in this online billion-dollar market, demanding more in exchange for their exposure.: An Experian study from January 2019 revealed that 70 percent of consumers from 21 countries are more willing to share personal data with organizations that offers a benefit such as convenience than last year[46]. The Center for Data Innovation conducted a similar survey in US and find that 58 percent of Americans are willing to share even the most sensitive personal data as biometric and location in return for the improvement of the online services they are used

[41] *Id.,* at 753.
[42] *Id.,* at 761.
[43] The total absence of free space to think and develop it, ending with the establishment of modulated democracies, as the information that reach us is increasingly biased. Cohen, supra note 29, at 13.
[44] Solove, supra note 40, at 767.
[45] Solove, supra note 40, at 766.
[46] PR Newswire (2019, January 29) - *70% of consumers would share more data if there was a perceived benefit, with greater online security and convenience at the top of the list.* Available at: https://www.prnewswire.com/news-releases/70-of-consumers-would-share-more-data-if-there-was-a-perceived-benefit-with-greater-online-security-and-convenience-at-the-top-of-the-list-300785756.html.

to handle[47]. Simultaneously, however, individuals have been expressing their concerns in sharing data[48].

We're facing a privacy paradox: whilst surveys as the ones above mentioned reveals that, having understood the market dynamic, consumers are comfortable in trading privacy for better services, others, as the released by ARF in March 2019[49], shows that the public would had become more aware of the risks of sharing massive information to privacy by affirming to hypothetical situations presented that they could be more reluctant in disclosing data – even though they still do not understand exactly why surveillance can be harmful or the privacy issues. When we look to the facts, people have been sharing in 2019 more data than in 2018[50], which shows us consumers would only value their privacy in abstract.

It can be the result of consumers being wronged by the terms of transactions in which they give up the secrecy of their information. Or, as pointed by Neil Richards, they also "might be coaxed by highly persuasive interfaces that use sophisticated testing models to be as effective as possible, or which limit their ability to make meaningful choices about their privacy[51]". It also may be the overconfidence we have that these companies which trade services for information are putting on our personal data. We still do not know exactly why, but personal data breach continues beyond people's awareness.

1.4. Privacy as fundamental right, not commodity

We entrust our personal information to a company whenever we buy online, believing that they have put adequate security in place to protect it, especially against cybercrimes. Unfortunately, this is not always the case, as huge data breach events in recent years have been showing us. About 57 million *Uber* global users, among customers and drivers, were exposed

[47] Center for Data Innovation, *Survey: Majority of Americans Willing to Share Their Most Sensitive Personal Data,* available at https://www.datainnovation.org/2019/01/survey-majority-of-americans-willing-to-share-their-most-sensitive-personal-data/.
[48] Marty Swant (2019, August 15), *People Are Becoming More Reluctant To Share Personal Data, Survey Reveals,* Forbes. Available at: https://www.forbes.com/sites/martyswant/2019/08/15/people-are-becoming-more-reluctant-to-share-personal-data-survey-reveals/#635b88471ed1.
[49] The Advertising Research Foundation - Findings from the 2nd Annual ARF Privacy Study. Available at https://thearf.org/category/articles/findings-from-the-2nd-annual-arf-privacy-study/#.
[50] Such analysis can be seen in greater depth in *We're giving away more personal data than ever, despite growing risks*, available at: https://venturebeat.com/2019/02/24/were-giving-away-more-personal-data-than-ever-despite-growing-risks/.
[51] Richards, Neil M., *Four Privacy Myths*. Revised form, "A World Without Privacy?" (Cambridge Press, Austin Sarat, ed. 2015), Forthcoming, at 15. Available at: https://ssrn.com/abstract=2427808.

to a data breach in October 2016 which compromised names, email addresses and mobile phone numbers[52]. *Equifax*, the third biggest credit firm in US, reported a cybersecurity incident which took place in July 2017 that affected information of 143 million consumers[53]. More than 150 million users of the *MyFitnessPal* app, owned by *Under Armour*, had personal information leaked in February 2018[54]. After multiples data breaches since August 2013, *Yahoo* disclosed in 2017 that all of its 3 billion email users were likely compromised by data theft, the record for largest ever data leak[55].

Besides such fails in protecting one's personal data, we had also threatening cases of consciously leaks, when information had been secretly shared by some powerful actors following promiscuous interactions between them. The most emblematic episode, in this regard, was the Facebook – Cambridge Analytica political scandal[56]. Cambridge Analytica was a British company that claimed to be able to analyze and combine huge amounts of data to identify and change, through behavioral science, providing targeted advertising and other data-related services to both political and corporate clients.

In early 2018 it was revealed that Cambridge Analytica had harvested the personal information of millions of Facebook users without their consent to apply in its business. Today we know that Facebook knew back in 2015 that such company had collected personal information on up to 87 million people. Yet, for more than two years, Facebook presented the risk of misuse of this data as hypothetical rather than warning the public about the leak, which hit the media only after a whistleblower disclosed the event details[57]. As it worked for the

[52] Julia Carrie Wong (2017, November 22), The Guardian – *Uber concealed massive hack that exposed data of 57m users and drivers*. Available at: https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack.

[53] Elizabeth Weise (2017, September 26), USA Today – *A timeline of events surrounding the Equifax data breach.* Available at: https://www.usatoday.com/story/tech/2017/09/26/timeline-events-surrounding-equifax-data-breach/703691001/.

[54] Hamza Shaban (2018, March 29), The Washington Post – *Under Armour announces data breach, affecting 150 million MyFitnessPal app accounts.* Available at: https://www.washingtonpost.com/news/the-switch/wp/2018/03/29/under-armour-announces-data-breach-affecting-150-million-myfitnesspal-app-accounts/.

[55] Verizon Media - *Yahoo provides notice to additional users affected by previously disclosed 2013 data theft.* Available at: https://www.verizonmedia.com/press/yahoo-provides-notice-to-additional-users-affected-by-previously/. More information about all the scandals, see Tech World - The most infamous data breaches. Available at: https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/.

[56]The Guardian, *The Cambridge Analytica Files*. Available at: https://www.theguardian.com/news/series/cambridge-analytica-files.

[57] Nicholas Confessore (2018, April 4), The New York Times – *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*. Available at: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html.

Trump presidential campaign, it is believed that Cambridge Analytica influenced other elections around the world, including 2018 Brazil running[58].

It is less of a question of whether people are willing to. Individuals are encouraged to share data in order to engage in basic services, to work or simply to stay connected in the modern world. People think it is worth it until they are individually attacked. Until there, our profiles have already been mapped, sold and used threatening our basic rights and determining even our political behavior. Privacy must be rethought not as information that can be kept totally secret, but as the question of what rules should govern the use of personal information, perhaps one of the most vital issue we face as a society today. Under these conditions, government interference through law thus is needed and have been executed as we will see next.

[58] An investigation was opened to investigate Cambridge Analytica's local partner, with no results to this date. Reuters - *Brazil prosecutors open investigation into Cambridge Analytica.* Available at: https://www.reuters.com/article/us-facebook-cambridge-analytica-brazil/brazil-prosecutors-open-investigation-into-cambridge-analytica-idUSKBN1GX35A.

CHAPTER II - IS THERE A GLOBAL DATA PRIVACY STANDARD ON THE WAY?

The past century history witnessed a large-scale government effort in collecting, cataloguing and even manipulating information on individuals[59], but gains in efficiency were considered more important than any privacy issues new technologies might generate[60]. An age of surveillance is in course[61]. These technologies that have revolutionized our routine have also conceived ever more detailed available data on our lives[62] and they have been updated in real time. Individuals Privacy, formerly managed almost exclusively by the state, is now controlled by big tech companies which make the sale of personal data a profitable business in a world where the concept of privacy itself is still poorly understood. This analysis thus will focus on the duties of such companies in collecting and processing such information.

Instead of the "race to the bottom" regular phenomenon on global trade, that is, the idea that countries will bring the current standards down in order to improve their competitive position, we are watching the opposite trend on data privacy regulation. In fact, domestic rules that govern some areas have become more rigorous with the steady global integration, in a truly "race to the top" law offer, as it happened to environmental law in a not distant past and has been occurring with data privacy regulation in the recent one[63]. Such preference for stringent law is more likely to be adopted by rich countries, rather than emerging markets, since only the first group have regulatory capacity either for creating good law and enforcing it, as well as can manage cuts in firms' profitability they headquarter through financial aid or partnership on behalf of data protection.[64]

The European Union has been the international privacy law protector pioneer. Since the GDPR came into force in May 2018, it consolidated itself as the world's privacy leading regulator driving and directing policy in the absence of another approach until very recently[65].

---

[59] Bignami, Francesca. *European Versus American Liberty: A Comparative Privacy Analysis of Anti-Terrorism Data-Mining* (April 18, 2011). Boston College Law Review, Vol. 48, p. 609-698, May 2007; Duke Law School Legal Studies Paper No. 135, at 610-611. Available at SSRN: https://ssrn.com/abstract=955024.

[60] J L. Riccardi, The German Federal Data Protection Act of 1977: Protecting the Right to Privacy?, 6 B.C. Int'l & Comp. L. Rev. 243 (1983), at 246. Available at: http://lawdigitalcommons.bc.edu/iclr/vol6/iss1/8.

[61] Richards, supra note 6, at 1936.

[62] *Id.*

[63]Bradford, Anu. *The Brussels Effect*, 107 Nw. U. L. Rev. 1 (2012), at 4. Available at: https://scholarship.law.columbia.edu/faculty_scholarship/271

[64]*Id*., at 11.

[65] See Bradford, supra note 63; Schwartz, Paul M.. *Global Data Privacy: The EU Way*, 94 New York University Law Review 771 (2019). Available at SSRN: https://ssrn.com/abstract=3468554; and Satariano, Adam. G.D.P.R.,

Perhaps US is the only country that still struggles to suit the European normative on data protection, at least until very recently. California, US richest state passed an act which goes into effect in 2020 that seems to inspire at least other 25 states[66] and, consequently, to end the tendency to reject EU law. The new Californian law, as it also increases the rights of individuals regarding their online privacy, resembles greatly the GDPR, at least at a first glance.

Few jurisdictions are powerful enough to influence domestic regulations outside their borders. In this chapter hence we will focus our analyses on the wealthier and main actors in the data consumer protection running, namely, EU and US, as well as their approach and prominent law (the GDPR and CCPA), to analyze whether a global data privacy standard can be observed.

2.1. The EU and US historical approach to data privacy

It is known that privacy in the market and public sphere has been better protected in Europe than in the United States. Rustad and Koenig tried to challenge such assumption showing that the E.U. and U.S. regulations with regard to data privacy are, instead, getting closer and closer.[67] According to them, despite some still relevant differences, there are a wide range of similarities and common inspirations among EU and US way to regulate data privacy protection. For example, the EU data rules always lack an effective enforcement mechanism, what got changed with the GDPR, which had this chapter truly inspired by US existing provisions[68]. Hence, it would be hasty to consider the European Union somehow ahead of the U.S. in terms of privacy protections[69].

Having nothing better than the past to explain the present yet history shows the opposite. EU countries and its people are in fact much more concerned with massive public

a New Privacy Law, Makes Europe World's Leading Tech Watchdog, N.Y. TIMES (May 24, 2018), Available at: https://www.nytimes.com/2018/05/24/technology/europegdpr- privacy.html.

[66] According to the National Conference of State Legislatures (NCSL) only in 2019, consumer privacy laws were introduced or filed in 25 states and Puerto Rico (Available at: http://www.ncsl.org/research/telecommunications-and-informationtechnology/consumer-data-privacy/calif.aspx.). Also, legislators in many US states proposed narrower privacy laws, as protection of biometric (More info at: https://www.uniformlaws.org/newsandpublications/news.)

[67] Rustad, Michael L. and Koenig, Thomas H., *Towards a Global Data Privacy Standard* (September 11, 2018). Florida Law Review, Volume 71, Forthcoming; Suffolk University Law School Research Paper No. 18-16, at 3. Available at SSRN: https://ssrn.com/abstract=3239930

[68] Rustad and Koenig, supra note 67, at 5.

[69] Determann, Lothar, *Social Media Privacy: A Dozen Myths and Facts*. Stanford Technology Law Review, Vol. 7, 2012. Available at SSRN: https://ssrn.com/abstract=2298891.

databases than all the fifty US states together, whether it is governmental or private-sector. Although many states and an increasing number of Americans (at least half of them believe their personal information is less secure now than the last years) recognition that unrestricted treatment of personal information puts people's privacy and security at risk[70], the United States lack a particular law at the federal level to handle the collection and use of personal information. In fact, for most of the US States personal data collection, storage and use are only subject to regulation on banking and health sectors.

For Bignami, this uninterested approach persists most likely because Americans never had their personal records so dreadfully used as Europeans during World War II.[71] Census were conducted both in US and Germany at that time using the same data processors known as Hollerith machines, manufactured by IBM. In the name of a better managed society, the maximum information available about natural persons, such as nationality, native language, religion and profession, were collected[72]. However, in Germany, what was supposed to be done for the commonweal resulted in millions of deaths as such data was misused by the Nazi government. Even after the war ended, the state surveillance remained intact in the partitioned Germany, carried by the Stasi, East German secret police, which had carte blanche to screen mail, search people's homes and torture anyone considered doubtful according to the files they kept on people's information[73].

In response to the rising of the data collection capacity of electronic data processing and its latent dangers, the German State of Hesse, in the West German, enacted in 1970 the country's first modern data privacy legal act[74], followed by a Federal Data Protection Act enactment in 1977, which aimed to regulate the entire personal data processing field within Germany[75]. In 1983, the German Federal Constitutional Court thus declared the fundamental right of self-determination over personal data within the *Census Decision,* prohibiting the treatment of personal data unless statutory authorizations is given or with the data subject

[70] O'Connor, Luala. *Reforming the U.S. Approach to Data Protection and Privacy*. Available at https://www.cfr.org/report/reforming-us-approach-data-protection

[71]Bignami, supra note 59, at 609.

[72] See more at Black, Edwin, *IBM and the Holocaust: The Strategic Alliance Between Nazi Germany and America's Most Powerful Corporation.* Dialog Press, 2002.

[73]Waxman, Olivia B.. *The GDPR Is Just the Latest Example of Europe's Caution on Privacy Rights. That Outlook Has a Disturbing History*. Available at https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/

[74] See more at the Library of Congress, Onlyne privacy law: Germany. Available at: https://www.loc.gov/law/help/online-privacy-law/2012/germany.php.

[75] J. L. Riccardi, supra note 60, at 248.

consent[76]. Such decision became the cornerstone of the EU approach today, aimed to prevent any large-scale effort whether from the private or public sphere.

History so describes two apparently incompatible privacy procedures. On one side, a laissez-faire regime that has been showing little appetite for broad privacy legislation and reflecting in data privacy its individual autonomy guide sense, which prevails in US. On the other, the more interventionist EU approach, concerned with social-protection. Both completely disinclined to build together an international standard on data privacy so far.[77]A proof of such is that, among them, Americans and Europeans have always been negotiating bilateral agreements on data trade affairs.

This disinclination resulted in the "U.S.-EU Safe Harbor Agreement," signed in 2000, allowing, as accurately observed by Chander, Kaminski and McGeveran, the US inoculation against any catalyzing effect from EU data protection law.[78] After the National Security Agency's mass-surveillance programs was revealed by Edward Snowden, the Court of Justice of the European Union, in 2015, declared that such agreement no longer was valid grounded on the argument that US law did not ensure an adequate level of protection of personal data[79]. Following the promulgation of the GDPR and the US refusal to conform its law to the EU adequacy standard, a new compromise was signed and remains in force despite of consistent efforts to be suspended as its precedent. Called "EU-U.S. Privacy Shield", such agreement differs from the former as it demands for stricter process to the transfer of data to third parties, requiring third party to provide the same level of protection assured by the original company[80].

2.2.Unilateral regulatory globalization – Brussels and California effect

There are two ways to pursue global regulatory harmonization. First and more well-known, it can be done through multilateral harmonization, which involves political effort of two or more sovereign states discussing issues previously agreed and where regulatory convergence will attend common negotiated goals, resulting in international treaties or

76 Library of Congress, supra note 74.
77 Chander, Anupam; Kaminski, Margot E.; and McGeveran, William. *Catalyzing Privacy Law* (2019). Georgetown Law Faculty Publications and Other Works. 2190. Available at: https://scholarship.law.georgetown.edu/facpub/2190
78 *Id*., at. 28.
79 Judgment in Case C-362/14, Maximillian Schrems v Data Protection Commissioner.
80 See more at Cave, Brian, *A Side-By-Side Comparison of "Privacy Shield" and the "Safe Harbor".* Available at: https://iapp.org/resources/article/a-side-by-side-comparison-of-privacy-shield-and-the-safe-harbor/.

agreements among states[81]. Secondly, some rules also can be unilaterally regulated. The unilateral globalization of standards results from having a single state (or union of states in EU's case) being able to export its laws beyond its borders relying on market procedures. There is no negotiation or even choice option[82]. A global standard will be imposed by the nation that meets a range of conditions, absent any form of coercion by threat or sanctions impositions.

Anu Bradford identified the conditions under which a superpower regulator might take place. First, the foundation for said ability to exercise authority abroad over other jurisdictions depend massively on market power. Producers and services providers are willing to adopt standards granted by the largest markets to have access to them, seeking to raise the volume of export to such countries. The larger the ratio of exports to the country ruler relative to the (lenient) market of the exporter country, the more likely the phenomenon to take place[83]. Add to that a strong regulatory ability, capable of translating said market power into tangible weight, and inelastic targets, such as consumers, which will not respond with some abrupt move to more restrictive regulation. Finally, none of the conditions listed here will suffice if the domestic preference have no propensity for strict rules, allowing the government to exercise rulemaking power in this way[84].

Hence it is not by chance that in some areas, including privacy, it is the EU that gives the cards globally, in what is known as the "Brussels Effect". EU is the largest importer of goods and services worldwide and had its regulatory capacity highly developed with the maturity of its single market during the last decades. US meets both the market power requirement and the regulatory ability to promulgate and enforce rules. Yet unlike EU, essentially for historical reasons as described above, the predisposition to accept government intervention of American citizens and companies on private issues, such as personal data, is fairly lower. More than that, US power in regulating finds substantial constraint in its decentralized data privacy regulation.

In the presence of the conditions listed by Bradford, hitherto domestic rules will be performed by multinational corporations with no option other than to abandon such profitable market. Since the standardization not rarely is the least expensive alternative for multinationals if compared to the adoption of multiple models in different countries, these companies also have a financial incentive to uniform their overall internal rules, movement called by Bradford

[81] Bradford, supra note 63, at 4.
[82] *Id*., at 3.
[83] *Id*.., at. 11.
[84] *Id*., at 14-15.

as “de facto Brussels Effect”. Due to the regulation costs inherent, such trend does not stop there. Multinationals as Microsoft have good reason to want to impose costs on its competitors and will not last to start to pressure the governments where they have headquarters and branches to adopt similar harsh rules, called so “de jure Brussels Effect”[85].

Prior to Bradford, Vogel formulated a similar thesis with regard to the power that California wields over other US states in environmental regulation and consumer protection law. He called it “California Effect”: “the critical role of powerful and wealthy ‘green’ political jurisdictions in promoting a regulatory ‘race to the top’ among their trading partners”[86]. California, as EU, thus could be considered a super regulator to privacy as it congregates all the conditions to make unilateral regulatory possible in US, which in its turn have enough influence over relevant institutions and countries[87]. According to him, the Golden State has the largest economy in US (if it was a separate nation, it would be the fifth largest economy in the world) as well as the most people. In economic terms, it represents an enormous attractiveness as companies would rather absorb the cost of regulation before renouncing this market. Second, said “race to the top” is more likely to take place if a robust institution, as the U.S. federal government, supports the harmonization of standards across the different jurisdictions. Finally, the standards must be supported by regulated companies that wish to have their competitors in other jurisdictions charged as they are in their own and endorsed by the public interest.

2.3. GDPR versus CCPA

As we have seen, EU has been converted into a superegulator. This block is currently able to determine global market regulation concerning some trade issues, environmental and data privacy in a relevant degree with ability to greatly influence even superpower countries as US and Japan. And it does that from simply regulating its internal market as per its needs. Few disagree[88]. The divergent minority do not deny the influential capacity that the EU enjoys on such issue, instead they claim that the adequacy provision, emanated from the EU privacy law

[85] Bradford, supra note 63, at 6.
[86] See Vogel, David. *Trading up: consumer and environmental regulation in a global economy* (Harvard U. Press 1995).
[87] *Id.,* at 260-68.
[88] Chander *et al* agree that “the GDPR has been the dominant influence on both de facto and de jure spread of privacy law worldwide.” For them, however, this story is partially true as the United States represents an exception to this narrative due to “in practice the US states largely copied California.”

and its main weapon (together with the extraterritorial effects, as we will see below), never shaped the US rules as bilateral agreements have been the rule in their relationship[89]. For such authors, it is not the GDPR that is catalyzing the rise of debates and the unprecedented volume of legislative data privacy proposals at the state and federal level in US, but the California Consumers Protection Act of 2018[90].

Would that be true? Could the US really escape the enormous influence of European law after so many inert years protecting data privacy while the latter was notably developing it? Is there still room for the US to build its own data privacy identity in a global and interactive economy where so many important actors, as huge multinationals, have been already complying with the strict European privacy law? To respond to these questions a closer look at the GDPR, the most relevant EU regulation on this matter and the CCPA, the Californian instrument that will come into force in 2020, is necessary.

2.3.1. *GDPR Overview*

The European Union is a devoted priest of data protection. Largely because of historical reasons, as noted above, data protection has been acknowledged under the EU approach as a distinct fundamental right, as it is asserted in Article 16 of the Treaty of the Functioning of the EU, as well as in Article 8 of the EU Charter of Fundamental Rights. More than that, due to the necessity to harmonize the national laws of some member states in order to ensure a high level of protection and the free flow of personal data within the block, EU has been regulating it closely since the Data Protection Directive's enactment in 1995.[91]

Such Directive remained in force for more than twenty years. Yet its transposition into national laws established a diverse data protection framework among EU countries, along with the rising of the giant tech companies and the way they used to collect and treat data, led to the proposal of a new legislation.[92] After a long legislative negotiation process and a transitional period, the General Data Protection Regulation (GDPR), encumbered to provide a single set of rules for all EU member states, directly applicable under EU law, became fully applicable on 25 May, 2018.

[89] Chander *et al*, supra note 77, at 28.
[90] *Id.*, at 24.
[91] Handbook on European data protection law, 2018 edition, at 25-29.
[92] Handbook on European data protection law, 2018 edition, at 30-31.

The GDPR preserves the core principles, as transparency and purpose limitation, and the legal bases, including informed consent, already considered for its predecessor, while develops some stringent points and introduces new obligations. The extraterritorial applicability of the GDPR maybe constitutes the major new feature to the regulatory landscape of data privacy. In this regard, not only organizations processing personal data within the European Union will fall under the scope of the GDPR, as it used to happen in the pre-GDPR circumstances, but also non-EU enterprises when offering goods or services to EU citizens. It includes providers of social networks or any other organization monitoring the behavior of individuals inside the block, whether the processing takes place in the Union or not,[93] requiring from all the countries with business interests in Europe urgent (re)formulation of its rules. Due to the little time, it gave rise to a Brussels Effect wave.

Among other relevant changes, the attempt of the GDPR to strengthen enforcement has no equivalent within the EU. Only after the Regulation, European data subjects were empowered and have conquered rights such as the right to pursue individual damages through lawsuit against a supervisory authority[94] and controllers or processors[95], as well as class-actions, common concepts to the US tort law[96]. Wealth-based fines were also established and organizations in breach of GDPR now can be fined up to €20 Million or 4% of the annual turnover of the preceding financial year, whichever is higher[97], upgrading even more enforceability.

The informed choice still forms the base for GDPR[98]. In this regard, the conditions for consent were enhanced and, instead of long and vague terms and conditions, request for consent must be distinguishable from other matters and given in an intelligible and easily accessible form that highlights the purpose for data processing[99]. Besides, It shall be as easy to withdraw as to give consent[100].

[93] General Data Protection Regulation 2016/679 (GDPR), art. 3.
[94] GDPR, art. 78.
[95] GDPR, art. 79.
[96] Rustad and Koenig, supra note 67, at 54-55.
[97] GDPR, art. 83.
[98] Informed Choice is the current world standard to business's online data collection and use practices, according to which all the internet actors are demanded to provide enough information on its policies in order to enable visitors to come to sufficient knowledge of the practices and make a reasonable evaluation of what it seems to be the apparent risks and benefits of disclosing data. The term "choice" means that there is an available alternative to the public, which might agree or not after being informed exactly what they imply, typically by clicking on an "I agree" button.
[99] GDPR, art. 7.
[100] GDPR, art. 7.3.

2.3.2. *CCPA Overview*

While Europeans had such progress in just over two decades, in the absence of a federal framework except for the few sectors, little interest was shown for broader privacy rules across the Atlantic Ocean. At least until the discussions around the GDPR took shape, followed by the proposal of the California Consumer Protection Act (CCPA) a month later the European regulation took effect. California became the first U.S. state with a comprehensive consumer privacy law after it enacted the CCPA. Since January 1st, 2020, this new law became applicable to business conducted in California and also satisfies one of the following three requirements: has a gross revenue greater than $25 million; annually buys, receives, sells, or shares the personal information of more than 50 thousand consumers, households, or devices for commercial purposes; derives 50% or more of its annual revenues from selling consumers' data.[101] In its turn, the CCPA is committed to protect Californians consumers that are either residents in California for other than a temporary or transitory purpose or domiciled outside the state for a temporary or transitory purpose[102].

Despite being a state law, the CCPA has a potential extraterritorial effect and out-of-state merchants selling or planning to sell must consider it while recording data of California consumers, including companies worldwide. Such data, or rather this "personal information", is defined by the law as "information that identifies, relates to, describes, is capable of being associated with, or may reasonably be linked, directly or indirectly, with a particular consumer or household."[103] The CCPA also relies on transparency to create new rights. For instance, it allows consumers to know, upon request, the categories of personal information the business has collected on him or her[104]. In addition, before the collection of personal information, the law demands companies to inform the purposes it should be used[105]. A right to erasure also is provided in the CCPA[106], demanding from a business the deletion of any personal information collected from the consumer upon a request, unless exceptions apply.

[101] California Civil Code §1798.140(c).
[102] California Civil Code §1798.140(g).
[103] California Civil Code §1798.140(o).
[104] California Civil Code §1798.100(a).
[105] California Civil Code §1798.100(b).
[106] California Civil Code §1798.105, §1798.130(a) and §1798.145 (g)(3).

Even more important is the new – in America – right to refuse data sales. From 2020 on, consumers will be able to opt-out of sale of their personal information[107], including third parties that receives such information, unless "the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out[108]." Nevertheless the prohibition of discrimination, business will be allowed to charge some difference as consequence for the exercise of such rights. This amount must be related to the value provided to the consumer by the consumer's data or based on regular financial incentives offered to compensate the consumer for the collection and sale of his or her data[109]. Its enforcement is the CCPA most controversial topics, since it does not allow for private causes of action, delegating all the power to the California Attorney General's office[110].

2.3.3. *Convergences and divergences*

The CCPA is not a reproduction of the GDPR and the differences between the two statutes are significant. Yet most of the substantial elements of the former are reproduction of important aspects of the latter, which brings considerable innovations to the existing US data protection law. For instance, because the Federal Trade Commission focuses its operation on the relationship between companies and consumers, it has no competence over the activity of data brokers who act like third parties. The CCPA thus is the first US law that brings data protection values without being narrowly sectoral, allowing, in our example, the directly investigation of data brokers regardless their commercial relationships.[111]

The GDPR delivers a broad definition of personal information, regulating data that renders a person identifiable in addition to information that precisely identifies him or her[112]. The CCPA follows the same direction and applies to information that can be directly or indirectly linked to a consumer or household, providing an open list of examples[113], like the GDPR does. These two laws detain the capacity to surpass its own jurisdiction to irradiate effects in others, following what we described before as the Brussels and California Effects.

[107] California Civil Code §1798.120(a).
[108] California Civil Code §1798.115(d).
[109] California Civil Code §1798.125.
[110] California Civil Code §1798.155.
[111] Chander *et al*, supra note 77, at 14.
[112] GDPR, art. 4(1).
[113] California Civil Code §1798.140(o)(1).

Either CCPA and GDPR have the transparency principle as their core foundation[114]. It means giving people notice and access rights to enable them to follow and in certain way to control their data. In this sense, the collection and purpose of processing, as well as the classes of information gathered and the existence of related individual rights, shall be disclosed to consumers. More than that, both regimes guarantee individuals' access rights, through which individuals are able to request collected and processed information at any time and businesses have to attend it promptly.

Other CCPA move totally in line with the GDPR is the adoption of a number of additional individual rights, which only differ in details, but essentially provide the same content. The provisions related to the right to data portability, for example, are very similar in the two statutes, ensuring one the right to receive his or her personal data in readable format and transmit those data to another entity.[115] The same applies to the right for individuals to opt-out, as both statutes encompass it. Yet the CCPA is more concise when allowing consumers to prevent a business to sell their data, while the GDPR has broader rights to opt-out on three analogous fronts: the right to restrict and object data processing, and to withdraw consent. The right to erasure, also called right to be forgotten, a still polemic introduction of the GDPR, is also provided in the CCPA as a narrower right to deletion, being applied only to business that directly collect the data from the consumer differently from the European statute.[116]

Besides the convergences, however, some substantive divergences are noteworthy. The GDPR deals with privacy, including in the data protection context, as a human right, while the CCPA holds its framework one step behind. Meaning, in practical terms, that, the Californian rule does not protect, as GDPR does, individuals in every situation concerning personal data processing. Rather, it focuses on the protection of consumers only in their dealings with business and regarding data just incidentally[117]. Such different approach to privacy treatment leads to divergence in the scope of some duties and rights. For instance, the CCPA allow for the collection and use of personal data unless a specific rule restrict such activities and only provides *a posteriori opt-out* mechanism. Unlike the GDPR, which is built around the concept of lawful processing of data, which means that personal information cannot be processed as a rule, but as exception according to one of the six grounds under article 6. Also,

[114] See GDPR, articles 14(1)(d) and 15; Cal. Civ. Code §1798.100(a) and §1798.110(a).
[115] See GDPR, article 20; Cal. Civ. Code §1798.100(d).
[116] Chander *et al*, supra note 77, at 16-18.
[117] *Id.*, at 18-19.

even when the processing is legitimized by consent and it is in accordance with the law's list, the GDPR considers additional principles to make its basis.[118]

The purpose limitation, data minimization and data retention are so important to Europeans as the transparency principle, but still means little in the CCPA which requires companies to disclosure data proceeding only if it is using personal information collected for additional purposes, but seems not concerned to stop it.[119] The treatment of individual rights is another good example of the consequence of having different approaches. Finally, though both laws contemplate monetary penalties in case of non-compliance, the enforcement mechanisms are also relevantly different. While the GDPR grants administrative fines to be issued by the national data protection authority, the CCPA mention civil penalties to be pursued by the California Attorney General office[120]. The amount provided by such laws also varies, from up to 4% of a company's annual global revenue to a maximum of $7,500 per violation in the GDPR and in the CCPA respectively[121]. Besides, the latter disregard the private right of action, except for a quite reduced set of claims, which in its turn constitutes one of the most celebrated innovations brought by the GDPR framework.[122]

3.4. Do we have a winner in the global trend running?

Yet change is now on US's doorstep. After the entry into effect of the GDPR, the main players headquartered in US, most of them EU export oriented, giant techs like Facebook and Google, were obliged to opt between changing its use and collection of personal data policies or abandoning the European market. These companies thus never had better incentive to break the ice and enhance its privacy compliance forces than the GDPR. Besides, public animosity towards technology companies has been promptly growing in the last two years[123].

Until 2018[124], when the GDPR came into force and the CCPA was enacted, the US government committed few efforts to protect data and its Congress has failed to build an identity

[118] Chander *et al*, supra note 77, at 19.
[119] Cal. Civ. Code §1798.100(b).
[120] Cal. Civ. Code §1798.155(a),
[121] See GDPR, article 83; and Cal. Civ. Code §1798.155(b),
[122] GDPR, article 79.
[123] See, e.g., Foroohar, Rana, *Year in a word: teclash*. Financial Times. Available at: https://www.ft.com/content/76578fba-fca1-11e8-ac00-57a2a826423e
[124] In 2018 and 2019, unprecedented legislative proposals regulating data privacy were presented at the state and federal level. See Kerry, Cameron, *Breaking down proposals for privacy legislation: How do they regulate?*:

American privacy law[125]. Indeed, before GDPR, a deregulated movement solidly linked to the US historical approach, considering also the freedom of speech discourse, preponderated against personal data protection[126]. The CCPA renewed the debate and has been changing the whole scenario in US as its richest state decided to treat personal information more carefully and broadly through a new law that encompasses all Californians consumers even the ones domiciled outside the state temporarily. Just as it happened with the GDPR, companies are engaged in complying with this new law to be able to address their products and services to California forty million people market.

Instead of fight against the GDPR or refusing its rules as the most efficient in terms of data protection, the CCPA confirms the importance of the first. Some differences exist, including some important divergences in approach, whilst there are important similarities among them. As stated by Schwartz, the CCPA enactment has proven that the EU-style data protection constitutes an appealing idea to be adopted by a large number of jurisdictions[127]. At the end of the day, the CCPA is highly inspired by the GDPR, even though it brings a less stringent rules and its own way to treat data protection.

For Rustad and Koenig the GDPR is actually a hybrid legal instrument that adopts massively from long established American privacy norms and remedies, as when endorsing privacy by design, US style enforcement, wealth based punishment and data breach notification[128]. Still according to them, such laws are in fact compatible and a global standard is at work, starting with the GDPR[129]. The extraterritorial impact of the GDPR thus would be unlikely to lead to any kind of data war and, indeed, no real battle between US and European law is detectable.

Privacy law in America faces what Hartzog and Richards call a "constitucional moment", that is, a period of constitutional transformation marked by intense public deliberation and participation[130]". American concern has become not only diminish the

Available at: https://www.brookings.edu/research/breaking-down-proposals-for-privacy-legislation-how-do-they-regulate/

[125] See, e.g., Hartzog, and Richards, supra note 26.

[126] See more at Jozwiak, Magdalena, *Balancing the Rights to Data Protection and Freedom of Expression and information in the EU: The Vulnerability of Rights in an Online Context* (June 1, 2016). Available at SSRN: https://ssrn.com/abstract=3138296; and Youm, K. H., & Park, A., *The "Right to Be Forgotten" in European Union Law: Data Protection Balanced With Free Speech?* Journalism & Mass Communication Quarterly, 93(2), 273–295.

[127] See, e.g., Schwartz, supra note 65.

[128] Rustad and Koenig, supra note 67, at 78.

[129] *Id.*, at 88.

[130] Hartzog and Richards, supra note 26, at 7.

exposure to the EU regulatory power[131] but also to take advantage of the Brussel Effect of the GDPR to confront the question of privacy law and create its own identity[132]. However, despite of the huge effort of US states in the last two years in approving new laws regarding data protection, at the federal level, none proposal bill seem close to come into effect[133].

Thus, if there was a race we could easily assert that Europe has been winning this for many years having as its main contributors the extraterritorial approach, a powerful adequacy norm and heavy diplomatic efforts. Besides, EU has benefited from developing concepts and legal model that have proved successful in a global marketplace of ideas[134] and has been persuading other countries to adopt its policies, either through the power of the GDPR, its ability to negotiate its terms or the gap left by other superpowers as the US.

[131] Bromund, Theodore, *The U.S. Must Draw a Line on the EU's Data-Protection Imperialism*. Available at: https://www.heritage.org/government-regulation/report/the-us-must-draw-line-the-eus-data-protection-imperialism.
[132] Hartzog and Richards, supra note 26, at 8.
[133] The already presented bills have been slowly processed and new ones are constantly proposed. See more at: https://threatpost.com/federal-data-privacy-bill-tech-giants/150663/.
[134] Schwartz, supra note 65, at 803.

CHAPTER III - THE BRAZILIAN GENERAL DATA PROTECTION ACT

The year of 2018 was tremendous for privacy and data protection laws, with a significant number of relevant privacy law developments worldwide. The end of the GDPR's implementation period, the introduction of an extensive privacy legislation in India and an increasing US effort at the federal and state level to strong its personal data proceeding rules might be remembered as the most relevant. Following such global trend, a General Data Protection Act was also approved in Brazil (called in Portuguese *Lei Geral de Proteção de Dados* – "LGPD") on August 2018[135] and is supposed to come into effect on January 2022[136].

The establishment of a new legislative framework to develop the country's legal system according to the challenges arising from technological developments has been on the Brazilian agenda for the last decade. A legislative tripod was conceived as government's initial plan with the update of the Brazilian Copyright Law[137] and the introduction of two new laws to regulate, respectively, Internet main aspects and personal data treatment[138]. In this sense, draft bills to reform copyrights rules[139] and create a Brazilian framework for internet issues[140] were firstly presented thus to the Congress, but only the latter was enacted in 2014 thanks to Edward Snowden who made public the US spying on Brazil's former President, Dilma Roussef.

Although personal data protection is not new to the Brazilian legislator with some dispersed legal instruments already treating such matter[141], Internet brought it back to light. A specific law to deal with it sufficiently and to list Brazil as granting an adequate level of protection for the processing of personal data was demanded. Fortunately, again, international circumstances, such as the GDPR and the Facebook/Cambridge Analytica scandal, speeded up entry into force of the Brazilian General Data Protection Act in 2018.

It is not uncommon to hear in Brazil that a law "will not catch on". Either because compliance will require efforts and investment that are known beforehand that it will not be

---

[135] Brazilian General Data Protection Act, Law No. 13,709/2018 (LGPD).

[136] According to the first version of the law, such rules would take effect in February 2020, but a new law extended it by 6 months. Due to the coronavirus pandemic LGPD was newly rescheduled to entry into force in January 1, 2022.

[137] BRAZIL - Law No. 9,610/98.

[138] Parentoni, Leonardo and Souza Lima, Henrique Cunha, *Protection of Personal Data in Brazil: Internal Antinomies and International Aspects* (March 30, 2019). International Conference on Industry 4.0 and Artificial Intelligence Technologies – INAIT 2019, at 3. Available at SSRN: https://ssrn.com/abstract=3362897.

[139] BRAZIL. Câmara dos Deputados. Bill No. 3.133/2012. Available at http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=534039; and Bill No.. 4.072/2012. Available at http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548155.

[140] Law No. 12,695/2014.

[141] Brazilian Federal Constitution, article 5º, IX, X, XI, XII e LV, and the Brazilian Criminal Procedure Code, article 201, §6º.

done or because, given the local culture, people will choose to keep going without following the new law and the authority is condescending to remain well esteemed before people. In this case, this possibility is remote, mainly because an effective data protection law is a requirement for Brazilian companies to continue receiving data from foreign individuals without bureaucratic obstacles. More than that, although the LGPD is not yet in force, two recent cases evidence that the protection system provided for the new law is already beginning to be effective through the application of the current legislative framework, namely, the Brazilian Civil Rights Framework for Internet and Consumer Protection Code[142].

As we will see, this new law represents a profound development in the way data privacy is treated in Brazil and to its international image as a country which provides satisfactory protection to privacy. For the first time, data subjects will be able to enjoy broad control and autonomy over their personal data, which may only be collected, used, processed and stored by either the state or a company under the strict rules imposed by the LGPD.

3.1. Ten principles to follow

Principles are the basis of the legal norm and the foundation of any legal system. In the words of Miguel Reale, a Brazilian jusfilosopher, principles "are normative statements of generic value, which condition and guide the understanding of the legal system, the application

[142] Special Appeal No. 1.758.799/MG debated whether the existence of a database without the consumer's knowledge would constitute harm and moral damage for violation of duty of information. The Brazilian Superior Justice Court held, in this case, that the management of the database imposes the observance of the rules requirements, which has the duty to communicate (as part of the duty of information) in writing to the consumer the registration and record of personal and consumption data when not requested by him. Ministers conclude that the sharing of consumer information by databases, although legally authorized, must respect the right of the registered to be informed in advance about the identity of the manager and about the storage and the purpose of the processing of personal data, as provided by the same law. Another interesting example of the LGPD principles assumption is the decision held by the Brazilian Department of Consumer Protection and Defense (DPDC) at the end of December 2019 (Technical Note No. 32/2019/CGCTSA/DPDC/SENACON/MJ. Case No. 08012.000723/2018-19) which sentenced Facebook to a fine of R$6,600,000.00 (around $1,500,000.00). DPDC is a body that assists Consumer National Secretary in the execution of the National Policy on Consumer Relations Consumption in Brazil and the administrative process concerns the famous Cambridge Analytica case and its consequences, in view of the suspicions of the misuse of Brazilian citizens' data. For such agency, the instant sharing of information from users who joined Cambridge's application and its friends on Facebook resulted from an opt-out mechanism, instead of opt-in. The number of people potential affected in such case would have been limited to eighty-four users or a quantity not much higher than that (precisely those Brazilian users who subscribed the app) in a opt-in system, rather than around four hundred and forty thousand. In this sense, DPDC considered that the Facebook's liability could not be dismissed and it would be up to Facebook to prove that such data were not unduly shared with those responsible for Cambridge Analytica, especially because, given the adopted opt-out model, it is the platform that had greater ability to monitor app developers' activities.

and integration or even for the elaboration of new standards.[143]" Principles inspire the creation of the norm, instruct the lawmaker about its motives and serves as assumptions demanded by the needs of research and praxis. In this regard, the processing of personal data under the LGPD is guided, basically, by ten principles, namely: finality, adequacy, necessity, transparency, unrestricted access, accuracy, security, prevention, non-discrimination and accountability[144].

Based on them, personal data processing with generic or indeterminate purposes will be no longer possible after the LGPD comes to force. The treatment of each personal information must be based on specific, legitimate, explicit and informed purposes, which cannot be modified during the treatment without a new consent. These purposes must also be within the limits of the law and must be provided together with all relevant information. In addition, the personal data processed must be compatible with the purpose informed by the company and only data strictly necessary for processing agents to achieve their purposes will be used.

Data subjects must be guaranteed that the information that processing agents have on them is accurate and up to date, to which the data subject must have free access, simply and free of charge. In this regard, all information provided by controllers and processors must be clear and precise. Furthermore, personal data can never be used to discriminate or promote abuse against its owners.

Constitute company's duty to seek procedures, means and technologies that guarantee the protection of personal data from access by third parties, including situations in which they are not authorized, as in cases of hacker invasions, correctively and preventively. Per LGPD, measures to solve accidental situations, such as destruction, loss, alteration, communication or dissemination of the personal data of its bases, must be taken thus by processing agents. Otherwise, in case of violations of the law and possible exposure of individuals, the LGPD, as we will see below, provides individuals with a cause of action to seek civil damages for such violations.

3.2. Individual's rights and processing agent's obligations under the LGPD

Hence, based on its founding principles, any law must provide rights and obligations addressed to those group which this law intends to manage their interrelation. The protection

[143] Reale, Miguel. *Lições Preliminares de Direito*. 27th edition. São Paulo, Saraiva, 2003, at 37 (Free translation from Portuguese).
[144] LGPD, art. 6º.

of personal data is inserted in the information society as a possibility to protect the individual in face of the potential risks that the treatment of data could cause to his/her personality. Rather to preserve the very data, the aim is to protect the data subject, who may have his/her right to privacy seriously affected while certain limits in the treatment of such data are not established[145], even damaging the democratic process at the end of the day, as we have seen.

Personal data, according to the LGPD, is information related to an identified or identifiable natural person. This includes information such as name, official documents and complex data such as geospatial information provided by your mobile phone's location service. It doesn't matter what the data is. If it concerns the individual, it belongs to him/her as an expression of his/her right to privacy and, in principle, it is private. To get access to it, data controllers must request permission from their owner who must assess the convenience of providing such data[146].

Whoever requests data in Brazil, in exchange for some facility or discount, being the LGPD in force, will be "processing" that data, which includes the collection, production, reception, classification, use, access, reproduction, transmission and storage, among other data-related activities personal. Under the LGPD, the basis and essential requirement for personal data processing is the data subject consent, expressly provided in a very clear manner[147], following the example of the new laws worldwide, including GDPR, except for the CCPA which does not demand for previous consent. It is true that the LGPD provides for 9 further hypotheses of lawful use of personal data in which consent is needless[148], yet, it is clear from reading such alternatives that consent will be the rule. Especially for companies.

Still, it is not possible to evaluate any data disclosure without being properly informed. The LGPD adopts thus transparency as one of its key principles of data processing, as guarantee to the data subjects of evident and easily accessible information. Data subjects have the right of access to information concerning the data processing of their personal data, including its purpose, duration and the identity of the controller. The right to be informed stands out among the most relevant[149]. Besides, such information must be stored in a format that favors access

[145] Mendes, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.* São Paulo, Saraiva, 2014, at 32.
[146] Sardeto, Patrícia. *Proteção de dados pessoas: conhecendo e construindo uma nova realidade.* Londrina, Gradual, 2011, at 52.
[147] LGPD, art. 8º, § 1º.
[148] LGPD, art. 7º.
[149] Note that, in this sense, the obligation to inform the purpose of the treatment has no exceptions in Brazilian law.

allowing data subjects to requested it at any time and free of charge[150] and the response may be provided, at the discretion of the data subject, in printed form, or by electronic means[151].

Operations using data must be strictly linked to the informed purpose[152]. If such purpose is no longer applicable, data treatment related to it have to be ceased. In case of its modification during the treatment, it will be necessary to request new consent[153]. Thus, only data that is strictly pertinent and necessary for the informed purpose should be treated. Also, the sharing of such data will depend on specific consent each time it takes place. Per this relevance, information about consent given to individuals by controllers must be quite clear. Lengthy and misleading terms and conditions will be considered null or void, pursuant to an extensive interpretation of the GDPR rather than expressly provided by the LGPD[154].

The personal data that individuals provide can serve as input to algorithms which perform personal, consumer or credit profiling and calculate decisions in an automated way that can affect the data subject interests. In these cases, LGPD guarantee to individuals the right to obtain information on the criteria and procedures used in the decision-making process, in addition to the right to request a review of those decisions[155]. Such law also provides for the right to portability meaning the portability of the data to another service or product provider, by means of an express request in accordance with the regulations of the national authority and provided that the transfer of data does not imply a violation of trade secrets.

Under the LGPD, individuals have the right to request deletion of their data in situations of unnecessary or excessive data, or data processed with the consent of the data subject. Data subjects will become entitled also, according to this new law, to rectify incorrect or incomplete data. Both rights will be exercised through request which must be answered immediately by processing agents, unless it is not possible under a reasonable justification. Besides, once the request is made, the processing agent who receives the request from individual must ensure that all other agents with whom it has shared the information to be deleted or rectified adopts identical measures[156].

Note, LGPD provides a right to the data subject whilst it imposes a correspondent obligation to processing agents regarding all the situations described above. In addition to such

[150] LGPD, arts. 6º, IV and 18, II.
[151] LGPD, art. 19, §2, I and II.
[152] LGPD, art. 6º, II and III.
[153] LGPD, art. 8, §§ 4º and 6º.
[154] Teixeira, Tarcísio. *Lei geral de proteção de dados pessoas: comentada artigo por artigo.* Salvador, JusPodivm, 2019, at 52.
[155] LGPD, art. 20.
[156] LGPD, art. 18.

obligations, controllers and processors have to comply to others equally or more important ones. Under the LGPD, for example, controllers and processors must maintain records of their personal data processing activities[157]. LGPD also demands from such actors the performance of a data protection impact assessment, documentation that must contain the description of the proceedings of personal data processing that could generate risks to civil liberties and fundamental rights, as well as actions, safeguards and mechanisms to mitigate such risk[158].

The new law also recognizes security as a fundamental principle of data protection and, in this sense, provides for duties and information security protocols that must be followed to guarantee the confidentiality of the personal data being processed. The LGPD states that controllers and processors must adopt security, technical and administrative measures able to protect personal data from unauthorized accesses and accidental or unlawful situations such as destruction, loss or alteration[159]. Besides any occurrence of a security incident that may create damage to the data subject must communicated by controllers to the National Agency and to the data subject itself. In the case of damage to privacy resulting from the processing of personal data, meaning both actual damage and risk of material damage, the data subject damaged will be entitled to ask for the liability of the processing agents involved, as well as indemnity[160].

3.3. Other relevant aspects: extraterritorial scope, cross-border data transfer and enforcement

In the internet age, a law that deals with data, personal or not, must consider the extraterritorial application of its effects in the effective protection of the data owner, since the data flow, for innumerous reasons, is not limited to a specific territory. The LGPD, fortunately, is one of those aware laws. Companies or individuals, all those who carry out collection and/or processing of personal data operations must comply with the new law, provided that the collection and/or processing is carried out in Brazil; that the treatment is aimed at offering goods or services in the national territory; or that the treatment relates to data from individuals located in Brazil[161].

[157] LGPD, art. 37.
[158] As provided in articles 5, 10 and 38.
[159] LGPD, art. 6º and 46.
[160] LGPD, art. 22, 42 and 45.
[161] LGPD, art. 3

For the personal data to be protected by the LGPD thus it does not matter the jurisdiction where the processing company has its headquarter, the location of the data and not even the nationality of its owner. It is enough that the data subject is located, permanently or temporarily, or the process is carried out in Brazilian territory. In this regard, even foreign companies that do not have representation in Brazil will be subject to the LGPD in one of these cases[162].

The issue of international data transfer between Brazil and other countries worldwide, especially those with which the country maintains strong commercial relations is also of great importance. After all, the flow of personal data is almost a prerequisite for business operations currently. The international perspective is directly linked to the protection ecosystem for personal data processing, as the absence of regulation can obstruct or make the business environment impractically expensive.

Consider cross-border data transfer from any European country (EU zone) to Brazil being carry out today. The GDPR requires additional guarantees to ensure competent protection in order to allow such transfer. These additional guarantees end up increasing costs and creating barriers to the free flow of data between the European Union and Brazil. And, due to the need for adoption of contractual arrangements or even the submission to certification processes services that could be provided by Brazilian companies to European Union companies become less attractive[163].

In the present context Brazil does not have a specific law dealing with international data transfer. The LGPD will change that, since such law designed safeguard mechanisms similar to those adopted by the GDPR to ensure personal data protection beyond the limits of their respective territories. Under art. 33 of the LGPD, international data transfer is only allowed in nine strict cases among with are the consideration of the degree of protection of the destination country, through specific consent of the holder, through guarantees offered by the controller or, still, through national cooperation agreement[164].

Regardless of its nature, every legal norm is constituted not only by the imposition of a conduct (positive legal order), but also by a sanction for the hypothesis of non-compliance (positive moral order). These two rules establish a cohesion according to which the perfect legal norm must necessarily have coercion as one of its fundamental element. The precepts that do

[162] Teixeira, supra note 23, at 34.
[163] Viola, Mario. *Transferência de dados entre Europa e Brasil: Análise da Adequação da Legislação Brasileira.* Available at https://itsrio.org/wp-content/uploads/2019/12/Relatorio_UK_Azul_INTERACTIVE_Justificado.pdf.
[164] Brazilian General Data Protection Act, Law No. 13,709/2018, art. 33.

not establish a sanction, in this sense, for the hypothesis of a violation of the legal norm would thus be incomplete propositions or mere auxiliary precepts[165]. Undeniable, in this regard, is that the effectiveness of any law is compromised if it does not include good enforcement mechanisms.

The LGPD, fortunately, is aware of this. The new law provides for the establishment of a centralized supervisory agency with corrective as well as investigative powers, called National Data Protection Agency (ANPD, in Portuguese)[166]. In this sense, the ANPD has power to request information, at any time, from processing agents and also corrective powers to issue warnings and fines as well as blocking or deletion of the processing or personal data to which the infraction refers. The ANPD will develop its own regulation on the criteria to apply and calculate such as financial and administrative fines, under the LGPD limits. Notwithstanding, the LGPD reserves individuals´ rights to claim civil damages (either financial or moral) due to privacy rights to be sought through individual or collective legal instruments before the Courts[167].

3.4. Consolidation of a standard law?

The comparison between LGPD, GDPR and CCPA is inevitable. Indeed, all these laws are contemporary, have several similarities and are dedicated to protecting the same right at the end of the day, that is, privacy. All such legal instruments are based mostly on the principle of transparency, through which the data subject has the right to choose, after being correctly informed, between to release or not his/her data do treatment in exchange for any convenience. In addition, the three laws allow the data subject to revoke consent, as well as ensure the right to correct and/or update data before provided. More than that, when we talk about GDPR, LGDP and CCPA, we are dealing with the flow of data through, at least, 6 of the largest economies in the world (considering California as a country).

The European Union General Data Protection Regulation took effect on May 25, 2018. One month later, California enacted the California Consumer Privacy Act. On July 27, 2018, India published a draft bill for a new, comprehensive data protection law[168] and, only a few

[165] Kelsen, Hans. *Teoria Pura do Direito*. 4th edition. São Paulo, Martins fontes, 2000.
[166] LGPD, art. 55.
[167] LGPD, arts. 22 e 42.
[168] Still in draft form. Available at http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf.

weeks after, Brazil followed with its data protection law on August 14, 2018. It is not a coincidence. EU choose privacy as its religion and has converted itself into a superegulator[169] able to determine data privacy rules globally, influencing even superpower countries as US after the latter remained many inert years protecting privacy. Historically, Europe was the first relevant market to be concerned about personal data protection, which is the result of years of personal data misuse by governments and big companies[170]. The GDPR is just the latest example of Europe's caution on privacy rights.

The CCPA has its own characteristics and important differences related to the GDPR. For instance, the CCPA are limited addressed to businesses that either have relevant revenue; buy, receive or sell personal information from more than fifty thousand consumers; or obtain fifty percent or more of the annual revenue from the sale of personal data. More important than that, CCPA subverts the logics of the GDPR when allowing for the collection and use of personal data unless a specific rule restrict such activities and providing *a posteriori* opt-out mechanism. Contrary to the GDPR, which requires a legal basis to be identified in order to process personal data. Yet, such specificities do not hide the moment that the CCPA was enacted, right after the entry into force of the GDPR, as well as the principles and motivations it brought from the latter. The same is true for LGPD which, despite some little inconsistencies in details, is very close to the GDPR.

Both laws are fairly consistent regarding personal, territorial and material scope, bearing a high degree of similarity in the rationale and differing only as to the details governing its application. In this regard, both the GDPR and the LGPD apply to organizations that have a presence in their territory and organizations that are not physically located in such jurisdictions, but sell their services or goods, or treat personal data in such places. Yet only the GDPR applies to organizations that monitor the behavior of individuals in the EU regardless any presence in there. Besides, both laws apply to the personal data treatment as carried out by controllers and processors, not only specific kind types of business per the CCPA. This principle is explicitly included in the GDPR, while in Brazil it is provided for by systemic interpretation, but, in both cases, it has the same finality, that is, protecting individuals aside from their nationality or residency status. They also both exclude from their scope the processing of anonymized data.

The GDPR as well as the LGPD are built around the concept of lawful data processing, meaning that personal information must be treated as exception and only if in accordance with

[169] Brussels Effect.
[170] Note, some of the most relevant companies had their boom when they started to working with the state machine, as we pointed at Chapter II regarding IBM.

one of the legal grounds they provide for. This directly impacts the possibility of data selling to the extent that, under both laws, the sale would only be valid if supported by legal provision and expressly consent from the data subject. One of the legal grounds provided for both GDPR and LGPD is consent, that is, when the data subject, after being correctly informed, gives his/her permission expressly.

On the other hand, in situations like that, the CCPA operates in completely reverse logic. Under the Californian Act, the personal data sale is allowed provided that the data subject does not expressly object it, regardless either any law provision or consent. Specifically regarding consent, the data subjects are entitled to opt-out, but are not required to opt-in. This difference demonstrates the idea of privacy adopted by each law. In Brazil, such as in Europe, privacy is a fundamental right. In the United States, however, privacy is interpreted as a commodity subject to free commercialization. When it comes to enforcement, the differences continue to accentuated. The CCPA does not provide for a data protection authority, as the GDPR and the LGPD does, meaning that the task to promote investigation is solely up to the Attorney General, the same legal body in charge for assess and issue civil remedies in case of non-compliance, since the CCPA does not provide for individuals with a cause of action to seek civil damages.

Individual's rights under GDPR, LGPD and CCPA are basically the same apart small differences, with the three laws being based on transparency and giving individuals rights to access and delete their personal data. The same applies to the obligation for treatment agents to maintain a record of the activities under their responsibility, provided for by these three laws, despite more or less prescriptive requirements brought by each. Yet the whole scenario is different regarding other obligations. Whilst the LGPD and the GDPR recognize the concept of adequacy and provide for the transfer of personal information to other countries or international bodies only on specific and limited grounds, the CCPA does not restrict the transfer of personal data outside the US. This also applies to the Data Protection Impact Assesment (DPIA), since both LGPD and GDPR require the conduction of impact assessments in order to assess processing activities risks to data subjects rights, while under the CCPA this duty is not mandatory.

Based on all of the above, it becomes clear the LGPD´s inspiration comes entirely from the European law. More than that, based on the time the CCPA was enacted, such as most of its provisions and basic principles, we would risk to say yes so, the GDPR is the basis for the Brazilian Act, to the Californian Act and probably to any legal system treating personal data

protection worldwide. After all, as we saw, European Union was the first block of countries to realize the necessity to legally regulate this issue and, after some years, to comprehend that it had the power to spread its regulation all over the world. The CCPA has its own characteristics and there are American scholars[171] talking in a law totally different from the GDPR. But it is not true. California has the power to disseminate its root over other American States and will do that. At the end of the day, however, it will be all.

[171] Rustad and Koenig, supra note 67.

CONCLUSION

Privacy is a complex value engorged with various and distinct meanings. Because of that, its concept remains unclear to most people. Selected surveys reveal that whilst individuals have been expressing their concerns in sharing data, ironically, they are more willing to increase their exposure in exchange for new benefits. The good news is that the personal data protection, as a consequence of the individual's right to privacy, has been part of the agenda and its relevance has increased on the international stage among lawmakers and scholars.

Amongst democratic governments there is unanimous perception that data protection calls for specific regulation. Even so, such governments did not demonstrate a willingness to pursue global regulatory harmonization through political effort in delivering multilateral agreements and international treaties in last years on this subject. Instead, what we have observed was unilateral regulatory globalization on data protection promoted by EU, resulted from its capability to export the GDPR beyond its borders either because the extraterritorial approach adopted, the powerful adequacy norm as provided or the gap left by other superpowers as the US over the years.

Due the benefits of harmonization and consistency with the EU model, many nations have moved to adequate their rules, among which Brazil, on data protection. Truly inspired by the same principles and having its individual’s rights and processing agent’s obligations in complete harmony with those provided for the GDPR, the LGPD consolidates the EU model on data protection and contributes for the same become the global standard on personal data privacy. In this regard, companies headquartered in Brazil already in compliance with the European Union rules must have much less work on implementing the LGPD and therefore to keep their business flow with EU regularly or even making it stronger.

BIBLIOGRAPHY

Bignami, Francesca. *European Versus American Liberty: A Comparative Privacy Analysis of Anti-Terrorism Data-Mining* (April 18, 2011). Boston College Law Review, Vol. 48, p. 609-698, May 2007; Duke Law School Legal Studies Paper No. 135, at 610-611. Available at SSRN: https://ssrn.com/abstract=955024

Black, Edwin, *IBM and the Holocaust: The Strategic Alliance Between Nazi Germany and America's Most Powerful Corporation.* Dialog Press, 2002.

Bradford, Anu. *The Brussels Effect*, 107 Nw. U. L. Rev. 1 (2012), at 4. Available at: https://scholarship.law.columbia.edu/faculty_scholarship/271

BRAZIL - Brazilian General Data Protection Act, Law No. 13,709/2018 – Available at http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

_____ - Law No. 9,610/98 – Available at http://www.planalto.gov.br/ccivil_03/leis/l9610.htm

_____ - Law No. 12,695/2014 – Available at http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm

_____ - Federal Constitution – Available at http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm

_____ – Criminal Procedure Code – Available at http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689compilado.htm

_____ - Câmara dos Deputados. Bill No. 3,133/2012. Available at http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=534039

_____. Bill No. 4,072/2012. Available at Available at http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=548155

Brooke Auxier *et al.* (2019, November 15), Pew Research Center, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*. Available at https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/

Bromund, Theodore, *The U.S. Must Draw a Line on the EU's Data-Protection Imperialism*. Available at: https://www.heritage.org/government-regulation/report/the-us-must-draw-line-the-eus-data-protection-imperialism

Cave, Brian, *A Side-By-Side Comparison of "Privacy Shield" and the "Safe Harbor".* Available at: https://iapp.org/resources/article/a-side-by-side-comparison-of-privacy-shield-and-the-safe-harbor/

CENTER FOR DATA INNOVATION - *Survey: Majority of Americans Willing to Share Their Most Sensitive Personal Data,* available at https://www.datainnovation.org/2019/01/survey-majority-of-americans-willing-to-share-their-most-sensitive-personal-data/

Cohen, Julie E., *What Privacy Is For*. Harvard Law Review, Vol. 126, 2013, at 1. Available at SSRN: https://ssrn.com/abstract=2175406.

_____, *Examined Lives: Informational Privacy and the Subject as Object*. Georgetown Law Faculty Publications and Other Works. 810. Available at https://scholarship.law.georgetown.edu/facpub/810

Confessore, Nicholas. (2018, April 4), The New York Times – *Cambridge Analytica and Facebook: The Scandal and the Fallout So Far*. Available at: https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

COURT OF JUSTICE OF THE EUROPEAN UNION - Case C-362/14, Maximillian Schrems v Data Protection Commissioner. Available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62014CJ0362

Determann, Lothar, *Social Media Privacy: A Dozen Myths and Facts*. Stanford Technology Law Review, Vol. 7, 2012. Available at SSRN: https://ssrn.com/abstract=2298891

EUROPEAN COURT OF HUMAN RIGHTS - Handbook on european data protection law, 2018 edition. Available at https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition

EUROPEAN PARLIAMENT - General Data Protection Regulation 2016/679. Available at https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32016R0679

Foroohar, Rana. *Year in a word: teclash*. Financial Times. Available at: https://www.ft.com/content/76578fba-fca1-11e8-ac00-57a2a826423e

Hartzog, Woodrow and Richards, Neil M., *Privacy's Constitutional Moment and the Limits of Data Protection*. 61 Boston College Law Review (Forthcoming 2020). Available at SSRN: https://ssrn.com/abstract=3441502

Jozwiak, Magdalena, *Balancing the Rights to Data Protection and Freedom of Expression and information in the EU: The Vulnerability of Rights in an Online Context* (June 1, 2016). Available at SSRN: https://ssrn.com/abstract=3138296

Kelsen, Hans. *Teoria Pura do Direito*. 4th edition. São Paulo, Martins fontes, 2000.

Kerry, Cameron, *Breaking down proposals for privacy legislation: How do they regulate?*: Available at: https://www.brookings.edu/research/breaking-down-proposals-for-privacy-legislation-how-do-they-regulate/

LIBRARY OF CONGRESS - Online privacy law: Germany. Available at: https://www.loc.gov/law/help/online-privacy-law/2012/germany.php

McGeveran, William. *Catalyzing Privacy Law* (2019). Georgetown Law Faculty Publications and Other Works. 2190. Available at: https://scholarship.law.georgetown.edu/facpub/2190

Mendes, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental.* São Paulo, Saraiva, 2014.

National Conference of State Legislatures (NCSL) - Available at: http://www.ncsl.org/research/telecommunications-and-informationtechnology/consumer-data-privacy/calif.aspx

Naughton, John, *The goal is to automate us': welcome to the age of surveillance capitalism.* Available at: https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook

O'Connor, Luala. *Reforming the U.S. Approach to Data Protection and Privacy*. Available at https://www.cfr.org/report/reforming-us-approach-data-protection

Parentoni, Leonardo and Souza Lima, Henrique Cunha, *Protection of Personal Data in Brazil: Internal Antinomies and International Aspects* (March 30, 2019). International Conference on Industry 4.0 and Artificial Intelligence Technologies – INAIT 2019, at 3. Available at SSRN: https://ssrn.com/abstract=3362897

Price, W. Michael. *Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine.* JOURNAL OF NATIONAL SECURITY LAW & POLICY. Vol. 8, at 11. Available at https://www.law.nyu.edu/sites/default/files/upload_documents/Price%20Rethinking-Privacy-Fourth-Amendement-Papers_2.pdf

PR NEWSWIRE (2019, January 29) - *70% of consumers would share more data if there was a perceived benefit, with greater online security and convenience at the top of the list*. Available at: https://www.prnewswire.com/news-releases/70-of-consumers-would-share-more-data-if-there-was-a-perceived-benefit-with-greater-online-security-and-convenience-at-the-top-of-the-list-300785756.html

Reale, Miguel. *Lições Preliminares de Direito*. 27th edition. São Paulo, Saraiva, 2003.

REUTERS - *Brazil prosecutors open investigation into Cambridge Analytica.* Available at: https://www.reuters.com/article/us-facebook-cambridge-analytica-brazil/brazil-prosecutors-open-investigation-into-cambridge-analytica-idUSKBN1GX35A.

Richards, Neil M., *Four Privacy Myths*. Revised form, "A World Without Privacy?" (Cambridge Press, Austin Sarat, ed. 2015), Forthcoming, at 15. Available at: https://ssrn.com/abstract=2427808.

_____, *Intellectual Privacy*. Texas Law Review, Vol. 87, 2008, at 416. Available at SSRN: https://ssrn.com/abstract=1108268

_____, *The Dangers of Surveillance*. Harvard Law Review, 2013, at 1934. Available at SSRN: https://ssrn.com/abstract=2239412

Richards, Neil M. and Hartzog, Woodrow, *Taking Trust Seriously in Privacy Law*. Stanford Technology Law Review 431 (2016), at 434. Available at SSRN: https://ssrn.com/abstract=2655719

Richards, Neil M. and Solove, Daniel J., Privacy's Other Path: Recovering the Law of Confidentiality. Georgetown Law Journal, Vol. 96, p. 123, 2007; GWU Law School Public Law Research Paper No. 249; Washington U. School of Law Working Paper No. 07-03-02. Available at SSRN: https://ssrn.com/abstract=969495

Rule, James B., *Privacy in Peril: How We Are Sacrificing a Fundamental Right in Exchange for Security and Convenience.* Oxford University Press, 2012.

Rustad, Michael L. and Koenig, Thomas H., *Towards a Global Data Privacy Standard* (September 11, 2018). Florida Law Review, Volume 71, Forthcoming; Suffolk University Law School Research Paper No. 18-16, at 3. Available at SSRN: https://ssrn.com/abstract=3239930

Sardeto, Patrícia. *Proteção de dados pessoas: conhecendo e construindo uma nova realidade.* Londrina, Gradual, 2011

Satariano, Adam. G.D.P.R., a New Privacy Law, Makes Europe World's Leading Tech Watchdog, N.Y. TIMES (May 24, 2018), Available at: https://www.nytimes.com/2018/05/24/technology/europegdpr- privacy.html

Shaban, Hamza (2018, March 29), The Washington Post – *Under Armour announces data breach, affecting 150 million MyFitnessPal app accounts.* Available at: https://www.washingtonpost.com/news/the-switch/wp/2018/03/29/under-armour-announces-data-breach-affecting-150-million-myfitnesspal-app-accounts/

Solove, Daniel J., *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*. San Diego Law Review, Vol. 44, p. 745, 2007. GWU Law School Public Law Research Paper No. 289, at 747. Available at SSRN: https://ssrn.com/abstract=998565

Solove, Daniel J., *Understanding Privacy*. Harvard University Press, 2008.

Swant, Marty. *People Are Becoming More Reluctant To Share Personal Data, Survey Reveals,* Forbes. Available at: https://www.forbes.com/sites/martyswant/2019/08/15/people-are-becoming-more-reluctant-to-share-personal-data-survey-reveals/#635b88471ed1

Schwartz, Paul M.. *Global Data Privacy: The EU Way*, 94 New York University Law Review 771 (2019). Available at SSRN: https://ssrn.com/abstract=3468554

Teixeira, Tarcísio. *Lei geral de proteção de dados pessoas: comentada artigo por artigo.* Salvador, JusPodivm, 2019

THE ADVERTISING RESEARCH FOUNDATION - Findings from the 2nd Annual ARF Privacy Study. Available at https://thearf.org/category/articles/findings-from-the-2nd-annual-arf-privacy-study/#

THE GUARDIAN – NSA Files. Available at https://www.theguardian.com/us-news/the-nsa-files

_____ - Available at https://www.theguardian.com/technology/2019/jan/20/shoshana-zuboff-age-of-surveillance-capitalism-google-facebook

_____ - The Cambridge Analytica Files. Available at: https://www.theguardian.com/news/series/cambridge-analytica-files.

UNITED STATES – California Civil Code. Available at https://leginfo.legislature.ca.gov/faces/codesTOCSelected.xhtml?tocCode=CIV

VERIZON MEDIA - *Yahoo provides notice to additional users affected by previously disclosed 2013 data theft.* Available at: https://www.verizonmedia.com/press/yahoo-provides-notice-to-additional-users-affected-by-previously/

Viola, Mario. *Transferência de dados entre Europa e Brasil: Análise da Adequação da Legislação Brasileira.* Available at https://itsrio.org/wp-content/uploads/2019/12/Relatorio_UK_Azul_INTERACTIVE_Justificado.pdf

Vogel, David. *Trading up: consumer and environmental regulation in a global economy* (Harvard U. Press 1995)

Wachter, Sandra and Mittelstadt, Brent and Floridi, Luciano, *Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation*. International Data Privacy Law, 2017. Available at: https://ssrn.com/abstract=2903469

Waxman, Olivia B. *The GDPR Is Just the Latest Example of Europe's Caution on Privacy Rights. That Outlook Has a Disturbing History*. Available at https://time.com/5290043/nazi-history-eu-data-privacy-gdpr/

Weise, Elizabeth (2017, September 26), USA Today – *A timeline of events surrounding the Equifax data breach.* Available at: https://www.usatoday.com/story/tech/2017/09/26/timeline-events-surrounding-equifax-data-breach/703691001/

Wong, Julie C. (2017, November 22), The Guardian – *Uber concealed massive hack that exposed data of 57m users and drivers*. Available at: https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack

Youm, K. H., & Park, A., *The "Right to Be Forgotten" in European Union Law: Data Protection Balanced With Free Speech?* Journalism & Mass Communication Quarterly, 93(2), 273–295.

Zarsky, Tal, *Incompatible: The GDPR in the Age of Big Data*. Seton Hall Law Review, Vol. 47, No. 4(2), 2017. Available at: https://ssrn.com/abstract=3022646

Zuboff, Shoshana, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. PublicAffairs, 2019