DOI: 10. /IJDL.magalhaes.v.2.n.2

Data protection regulation: a comparative law approach

Proteção de dados: estudo comparado de normas nacionais

Marcus Abreu de Magalhães*
Ambra University (Orlando, Florida, United States)
marcusmagalhaes@portalambra.com
https://orcid.org/0000-0002-9366-9007

Recebido/Received: 23.01.2021/ January 23th[rd], 2021
Aprovado/Approved: 17.08.2021/ August 17th, 2021

Abstract: This paper aims to present a comparative approach to data protection regulations around the world. Most countries possess data protection laws in some level of detail. In order to compare structures of data control and compliance in dissimilar systems, the study selected four distinct arrangements: the European General Data Protection Regulation (GDPR); the California Consumer Privacy Act (CCPA); the Brazilian Digital Privacy Law, *Lei Geral de Proteção de Dados Pessoais* (LGPD); and the Chinese Data Privacy Framework, which is molded by a set of different regulations. The analysis was based in common key points of those regulations – territorial scope, consent and disclosure, data security requirements, data transfer, Data Protection Officer, awareness and training, and penalties – to explore the different policies and national goals. The paper argues that, in the landscape of the information based society, new law is needed to protect citizens' rights to privacy and to bound harvesting and mining of personal information to ensure transparency, control, and compliance of the information economy.

Keywords: Data protection. Comparative law. Privacy. Information society. Data mining. Compliance.

Resumo: O trabalho busca apresentar abordagem comparativa entre normas de proteção de dados em diferentes países. A maioria das nações possui alguma norma para regular o tratamento de dados. Assim, com o propósito de comparar estruturas de controle de informações e de governança de dados, o estudo selecionou quatro modelos distintos: o Regulamento Geral de Proteção de Dados europeu (GDPR), o Estatuto de Proteção à Privacidade do Consumidor da Califórnia (CCPA), a Lei Geral de Proteção de Dados Pessoais do Brasil (LGPD) e o plexo de normas que compõem o modelo de proteção de dados na China. A análise partiu de pontos comuns dos diferentes sistemas jurídicos – abrangência territorial,

Como citar este artigo/*How to cite this article*: MAGALHÃES, Marcus Abreu de. Data protection regulation: a comparative law approach. *International Journal of Digital Law*, Belo Horizonte, ano 2, n. 2, p. 33-53, maio/ago. 2021.

* MSc in Legal Studies – AMBRA University. Bachelor's Degree in Law from Universidade de Brasília. Graduate in Economic Sciences from Universidade de Brasília. Specialist in Constitutional Review and Fundamental Rights (Pontificia Universidade Católica do Rio de Janeiro) and in Administrative Law (Universidade Gama Filho). State judge (State of Mato Grosso do Sul, Brazil).

consentimento e divulgação, requisitos de segurança, limites à transferência de dados, encarregado de proteção de dados, treinamento, sensibilização e sanções – para explorar os diferentes regramentos e objetivos nacionais. O estudo propõe que, no panorama da sociedade da informação, novas leis se fazem necessárias para assegurar a privacidade dos cidadãos e para balizar as atividades de mineração e extração de informações pessoais para assegurar a transparência, o controle e a governança na economia da informação.

Palavras-chave: Proteção de dados. Direito comparado. Privacidade. Sociedade da informação. Mineração de dados. Governança.

1 Introduction

Privacy rights have been in the spot with the rise of concerns regarding the abuse and misuse of personal data by governments and big data corporations. These concerns sparked a new set of rules related with dada compliance, control, and accountability. Nations have then sought to put in place a legislation framework to enforce data protection rights. Those general data protection regulations, despite their titles, are still confined in the jurisdiction of the lands or unions of nations where they can be imposed.

But, in order to be viable in a digital world with no borders (or fewer walls then those of the country's political divisions) those different set of rules should be the most compatible with each other as possible. As the corporation's extent disregard borders, any approach needs to assert the global scope of digital and virtual universe. Europe, USA, and China still have the economic power needed to impose data policies upon corporations. But smaller countries most probably will need to follow the guidelines settled by the large economic players.

The last decades witnessed a complete reorganization in the way humankind promotes the distribution of information. We are moving from a Propriety-based to an information-based society. This transformation means that the wealth generation, the economic activity, and the institutions awareness are turning to data gathering and control. The data mining, control and modeling shall be therefore crucial to human activities in this new environment.

The new social paradigm is changing the way people and institutions relate to themselves to incorporate the new power, value, and status core. After millennia with the hunter collector way of life, humanity has perfected techniques for growing crops and rearing animals. In the Neolithic Revolution we settled in cities, developed money, writing and everything changed.

The Age of Discovery, first led by the Portuguese with overseas navigations skills and then by the English with the Steam Power, also prompt new transformations

in the way we organize our societies. With the Industrial Revolution, new means of transportation, new frontiers and technologies, the world seemed to shrink and, again, everything changed.

The Industrial Revolution happened in two phases. First the mechanization, with railroads, steam machines, and then the electricity brought the assembly line and the automation. In the XX century, a third step was recognized by the transistor and the electronic innovations. But nowadays it seems that the electronic shift was the first step in an Information Revolution.

Some intellectuals like Klaus Schwab,[1] economist, founder, and director of the International Economic Forum, classifies the digital transformations as a fourth step in the Industrial Revolution. At the Hannover Fair he coined the term Industry 4.0 about the digital changes.

But maybe we are trending to a bigger picture. In the eighties, Alvin Toffler talked about an information-based way of living in his book The Third Wave.[2] The author had foreseen the e-commerce, digital payments, communications, and relevant details of what seems to be a digitally interconnected society. Before that, in the seventies, other authors commented about a Post-Industrial Society,[3] [4] but the transition to a cyber digitally driven society was pointed by Toffler in his next major work.[5]

In any form one chooses to describe it; the dawn of the information technology has permitted the transition to a new way of life. The global pandemic of Covid-19 in 2020 was a turning point for the affirmation of the new times or new normal with intense information technology use to maintain the business and personal routine in times of social isolation.

But, with the new technology, new problems had arisen. We face global cyber threats, new sorts of crimes and new ways to negotiate people personal data. Personal information has become a new commodity. And the bigger players in the game are in the personal data league. The five biggest US companies in the stock market – Google, Microsoft, Apple, Facebook, Amazon – deals with personal data and big data analytics. In a global perspective, others big players – Tencent, Huawei, Ali Baba, Baidu, Xiaomi – are also in the data business.

This new social structure calls for an equally new legal apparatus, especially for the protection of citizens privacy and individual rights. Several nations are working

1 SCHWAB, Klaus. *The Fourth Industrial Revolution.* New York: Random House LLC, 2017. p. 15.
2 TOFFLER, Alvin. *The Third Wave*. New York, USA: Bantam Books, 1980.
3 TOURAINE, Alain. *La société post-industrielle*: naissance d'une société. Paris: Denoël, 1969.
4 BELL, Daniel. *The Coming of Post-Industrial Society:* a Venture in Social Forecasting. Nova York, USA: Basic Books, 1973.
5 TOFFLER, Alvin. *Powershift:* Knowledge, Wealth and Violence at the Edge of the 21st Century. New York, USA: Bantam Books, 1990.

towards the objective to form a comprehensive body of law to regulate de cyberspace. But the matter is controversial, as the parties interested claim a cyber freedom or a deregulated virtual space as inherent of digital technologies and, beyond that, companies are putting their servers, teams and headquarters in more favorable jurisdictions or even putting data in international waters.

So, in one hand there is a need to protect the individual privacy and regulate the reach of those big data companies over citizens civil rights; and, in the other hand, the new cyber tools and data abilities seems to be far complex to be effectively overseen by regulators.

But the challenge is up most relevant because the correct distribution of risks and responsibilities linked to data compliance, personal information and individual rights will be crucial to promote better services, protection, and development.

2 Study problem and methodology

To what extent do the structure of the regulation and the organization of personal privacy policies and statutes differ in selected law systems.

The aim is to explore the hypothesis that although the statutes and regulations are oriented around similar points, the cultural and legal particularities of each system will matter the most in order to settle the guidelines of each national data protection policy.

The analysis is relevant because the global scope of data processing activities will be shaped by the diversity in legal approaches and orientations. Beyond the textual analysis of local statutes, a broad comprehension will be paramount to effectively access the range of personal data protection extent in different countries.

The study follows a qualitative and exploratory method because the recent data protection statutes still configure new laws pending court challenges and real cases tests. In order to tackle the problem we choose to compare the actual statutes and regulations and compare to a broad view of the different law systems where they are inserted.

In that context, in 2016, the European Union has approved the General Data Protection Regulation (GDPR), which, in 2018, has effectively replaced the Data Protection Directive 95/46/ec. The GDPR is now a comprehensive statute regulating how companies must protect EU citizens' personal data.

The United States does not have a federal regulation, nevertheless the Federal Trade Commission have settled the grounds to a federal approach with the Facebook FTC[6] settlement in 2019 and shall be further guidelines in the FTC anticompetitive

[6] Federal Trade Commission.

conduct complaint in 2020. In the meantime, the regulation should be shaped by each state.

California has already passed a regulation, the California Consumer Privacy Act – CCPA, to secure privacy rights for California consumers. Other States like New York, Washington, or Illinois have bills under analysis at the Legislative Committee.[7]

In fact, it is not yet clear if the privacy regulation will be enacted by states or if it will fit in the exception enumerated in the United States Constitution for the Union legislative powers by the Supremacy Clause. The nature of virtual and digital ecosystems could be potentially messy if each of different state establishes local privacy laws. This hodgepodge could be better addressed if the problem fits the Commerce Clause, the matter seems to fit particularly under the legal doctrine known as the Dormant Commerce Clause, but it will eventually be sorted out by the Supreme Court.

Brazil also passed a statute to secure privacy rights clearly inspired by the EU GDPR. The Brazilian GDPR statute – Lei Geral de Proteção de Dados LGPD – was passed in 2018 but effectively came into force in September 2020.

South Africa, Brazil's partner in BRICs international economic organization, also have a privacy statute – the Protection of Personal Information Act POPIA – which was ratified in November 2013 (before the EU adopted the GDPR), but progress subsequently hindered for several years until it finally came into force in July 2020.

Argentina, Uruguay, and Paraguay – Brazilian's partners in Mercosul – also have specific legislations about digital privacy. Argentina has passed the 25.326 law in 2000; Uruguay has passed a similar statute, the 18.331 law of 2008; and Paraguay the 1682 law of 2001 significantly reviewed by the 5543 law of 2015. As EU has digital privacy exigencies to allow foreign companies to operate in their borders, Argentina and Paraguay have successfully submitted their statutes to the European Commission, with approval on June 30, 2003 and on August 21, 2012, respectively.

And, in China, the Standing Committee of China's National People's Congress – NPC approved the *Decision on Strengthening Network Information Protection* in December 2012. And, last October, China unveiled its latest 2020 draft of the Personal Data Protection Law. The 2012 *Decision* (DSNIP) was the first equivalent of law in Chinese legal system expressly aimed to "protect network information security, protect the lawful interests of citizens, legal persons and other organizations" and "safeguard national security and the public social interest". Already in the first article it is possible to identify the Decision as a privacy law:

[7] In New York, the bill of State Senator Kevin Thomas, Senate Bill S5642; in Illinoi the Senate Bill 2330, by Senator Thomas Cullerton; and in Washington State the Senate Bill 628 was rejected, but there's a limited control regulation over biometric data.

> I, The State protects electronic information by which the individual identity of citizens can be distinguished as well as involving citizens' individual privacy.

No organization or individual may steal or obtain in other illegal manners obtain citizens' individual electronic information, sell, or illegally provide citizens' individual electronic information to other persons.

Overall, the nations of the world are looking for implement a vast array of digital privacy laws. The United Nations Conference on Trade and Development – UNCTAD registers 66% of the UN countries with some kind of privacy law and other 10% with draft legislations in the making. There are still 19% of UN countries without privacy legislation, and they have no data for the remaining 5%.[8]

The information access and manipulation can be harmful in several ways. In the international arena, the cyber threat has entered in the agenda since many attacks suffered by governments and private organizations. Those cyber-attacks have been delivered either by underground groups or rogue organizations on behalf of other nations or concurrent private companies. In fact, they have been an effectively instrument to steal corporate secrets, anticipate business strategies or to promote embarrassments to top executives.[9]

In the other hand the privacy rights violations can also happen accidentally, with the unintentional exposure of images, information, or metadata of private citizens, or purposely with companies willingly to sell private data for a diversity of purposes. In fact, the private data commerce is the main concern of those new privacy laws, as the rush for information gathering is the new gold rush for the XXI century.

All these new regulations create a set of obligations for the data providers and controllers, usually barriers to sharing personal data, rules, and deadlines to erase information; as well as an inventory of citizens civil rights, as the right to control which information will be available, which data the application provider can have, information about what has already been collected and the right to erase or rectify de registers.

The aim of this article is to exhibit the digital privacy laws of Brazilian's main commercial partners – China, United States, Europe, and Argentina – regarding companies' obligations.

---

[8] The United Nations Conference on Trade and Development website at: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. Accessed on 12 December 2020.

[9] For instance, the Sony cyber-attack before The Interview movie debut in 2014, it culminated in a scandal that cost the job of Amy Pascal the top executive in the entertainment branch at the Corporation.

3 European GDPR

The European GDPR is the key statute as it is the most comprehensive and detailed of the laws already in force. The European approach set those main obligations for the companies settled in their territory or offering services for their citizens, it means that in addition to EU based enterprises, any company that offers goods or services to EU residents, regardless of its country of origin, will be subjected to the EU regulation, as stated in the article 45 of the GDPR. Thereby, the GDPR has a global influence on data protection regulations models.

The main benefit for the Union is that the GDPR is able to impose a uniform data security law on all EU members, so that each member state will not need to create its own data protection system and the regulations will be consistent across the entire Europe.

The statute contains XI chapters and 99 articles. The following are some of the topics that have the greatest potential impact on security operations:

3.1 Territorial Scope

The GDPR applies to any organization that collects, stores, or processes the personal data of European residents. It does not matter if the organization is actually based in the EU.

3.2 Lawful, fair, and transparent processing

That means that all companies processing personal data must treat the information in a lawful, fair, and transparent manner. For the scope of the statute, lawful implies a legitimate purpose for all the data processing. One must assert a need to treat or archive the information collected. Fair also is related with the notion of good will and good practices; the companies will be responsible and will not process data for any purpose other than the legitimate ones. And finally, transparent means that the data subjects will be informed about the use, including third parties' access and repurposing, of their personal data.

3.3 Limitation of purpose, data, and storage

The companies will restrain the data gathering and limit the processing, collecting and data crossing only within the necessary extend for the revealed purposes, and discard personal data once the original objective is fulfilled. That implies those other requirements: i – not process personal data beyond the legitimate intent for which it was gathered; ii – no personal data other than necessary shall be requested; iii – all

the personal data must be erased once the legitimate and disclosed motive – for which the gathering was authorized – is attended.

3.4 Disclosure

When asked, the company shall disclose what information it has about the petitioner, and what the purpose and uses of this data. Also, the data owner has the right to demand correction, formalize a complaint, order the deletion, or ask for the transferring of the personal data. The articles 19 and 20 of the GDPR are aimed to ensure that one shall have control over his or her data. Under those provisions, one may demand a full deletion of his or her personal data (right to erasure) or request the right to transfer personal data between service providers (right to portability).

3.5 Consent

A clear and explicit consent must be obtained in order to collect or process personal data, article 6 (1) (a). And this consent may be withdrawn by the data subject without justification at any moment, article 7 (3). In order to process information of minors (under 16 years old) the data controller will require consent of the parents, article 8 (1).

3.6 Personal data breaches

The data controller will maintain a data breach register, and, in some cases of high severity, the public regulator and the data subject must be promptly informed. Article 33 of the GDPR rules that controllers must notify supervising authorities of personal data breach within 72 hours of learning of the leak and must provide specific details of the breach such as its nature and number of subjects affected. Article 34, in its turn, requires the controllers to also notify the victims “without undue delay”.

3.7 Privacy by Design

Business must incorporate in their projects, products, and systems technical mechanisms to protect personal data. The privacy by design means that the product or service will be planned to ensure the privacy rights of the consumers by default. Articles 23 (1) (i), 23 (2) (d) and 35 require private or public entities to implement data protection measures to protect consumers’ personal data and privacy against loss or undue exposure. Those measures must be reasonable, so it is not always a system of absolute liability over those safeguards.

3.8 Data Protection Impact Assessment

A Data Protection Impact Assessment is needed to initiate a new project or product. The Data Protection Impact Assessment shall be available for the Data Authority and also subjected to internal compliance. Article 35 requires companies to perform Data Protection Impact Assessments in order to identify risks and subsequently routinely Data Protection Compliance Reviews to ensure those risks are addressed. The Data Authorities may implement routine auditing to enforce its effectiveness.

3.9 Data transfers and data tracking

The company will have a controller officer with the duty to ensure that the personal data is protected under GDPR requirements, the company is liable as well if the processing is made in house or by a third party. This means that controllers will share the responsibility over personal data even when that data has been outsourced.

3.10 Data Protection Officer

When a certain criterion is met – for instance when there is significant volume of data; when the processing refers to genetic data, health, racial or ethnic origin, religious beliefs; or even when the company collect personal information about their own employees as part of human resources processes – the organization must designate a data protection officer. The article 39 states that those officers serve to inform and advise organizations about their obligations pursuant the GDPR regulations and act as a contact point with the Supervisory Authority [article 39 (1) (e)]. The DPO will also monitor compliance in all the data related sectors, article 38 (1) (b), and have direct communication with the higher administration, article 38 (3). The DPO can be hired outside the organization or be in their ranks.

3.11 Awareness and training

There is a permanent duty to promote GDPR awareness among the organization. The DPO has also to ensure awareness-raising and staff training, article 39 (1) (b). Those practices are not only relevant in regard to the protection of personal data but also for identify data breaches and vulnerabilities.

3.12 Penalties

Article 83 outlines the penalties for GDPR non-compliance, which can be up to 20 million Euros or 4% of the violating company's worldwide annual turnover of the preceding financial year, whichever is higher. Those penalties are among the higher between data privacy legislations around the world. Besides companies, data controllers and processors are subject to the supervising authorities' oversight and penalties.

4 California US – California Consumer Privacy Act (CCPA)

California passed, on January 1st, 2020, the first American data privacy law. California is the largest and richer state in the US and home to Silicon Valley and the major US technology enterprises. It is a wide-range data privacy regulation that was largely modeled on EU's GDPR. Because it is the first and because it is from California it will have a huge impact on the futures US statutes about privacy data.

It affects for profit organizations and companies that collect and use personal data about citizens of California. The CCPA is also requires companies to become more transparent about the data they collect and five consumers a certain degree of power over the data that will be shared.

4.1 Territorial Scope

The CCPA applies to any large for-profit organization that does business in California, intensely collects personal data about California residents or has the data collecting as main business. A CCPA covers the personal data provided directly by users in online forms and data collected by tracking tools and related technologies. The formal criteria are: i – It brings in annual gross revenues of at least US$25 million; ii – It collects personal information from 50,000 or more Californian residents, households, or devices per year; iii – It generates more than 50% of its annual revenue by selling personal information about California residents.

4.2 Disclosure and Consent

Businesses can process and sell personal data if they offer clearly option to opt out of such transactions. The CCPA has granted the right to California citizens to request the inventory of personal data stored about them. In addition, California residents can also request the deletion of their data. The controller must administer those requests free of charge.

4.3 Data Security

The CCPA does not have a specific requirement to enforce data security, the model seems to resolve the issue with private judicial action in the event of losses due to a data breach, the future judicial solutions will delimitate what will be the grounds for business reasonable measures and the security level needed to prevent such an event from occurring.

In that respect the CCPA don't have special requirements to control, contain or disclose data breaches to a specific agency.[10] Nor they require the products to enforce privacy by design.

4.4 Data Transfer

Consumers can opt out, i.e., ask for their data not to be shared with or sold to outside parties. Companies must delete all the data held on a Consumer upon request (with certain legal exceptions). And for enforce those requirements the controller is not allowed to modify the service levels or prices due to the Consumer invoking rights outlined by CCPA. And is worth to note that, unlike other systems, the CCPA does not limit the transfer of data outside of the US.

4.5 Data Protection Officer

Unlike the GDPR, CCPA does not require the appointment of a dedicated data protection officer, or any similar role (including a chief privacy officer, or CPO).

4.6 Penalties

The State of California will impose a civil penalty of up to $7,500 per violation on any company that is in breach of the CCPA and fails to address the requirements of the law within 30 days. In parallel the residents have the possibility to pursue damages of up to $750 per incident in the event of exposure.

In comparison with the EU GDPR, it's important to note that whereas GDPR gives data citizens the right to choose if companies can use their personal data for marketing purposes, CCPA opt-out rights are more concerned with the sale of personal data. There is no special provision to mass mail marketing (spam) or abusive advertising.

[10] The CCPA doesn't have specific data breach requirements. Another law regulates the subject: the California Data Breach Notification Law CDBNL. So, there will be certain circumstances where data breaches would be actionable according to this notification law.

Also, GDPR has rules about how data can be transferred, and it is not possible to transfer, process or store data outside of the European Economic Area (there is a list of exceptions). But, as a country with state-by-state data privacy laws, without federal regulation the US does not currently provide such protection. So, in order to American companies work inside the European Borders, they must operate inside the EU-US Privacy Shield framework.

5 Brazilian LGPD

Brazilian main Digital Privacy Law, *Lei Geral de Proteção de Dados Pessoais LGPD*, is remarkably similar as it was inspired from the EU General Data Protection Regulation. It aims to strength the data privacy rights of Brazilian residents and to comply with European requirements to international commerce, as it is mandatory in many aspects to ensure full benefits from the free trade deals between Mercosul and European Union.

As it was mentioned above, GDPR requires an adequate level of data protection (and it is evaluated by the European Commission) in conformity with Regulation 2016/679 EU and with article 45 of GDPR.

In that regard the statute is aimed to ensure best practices and compliance. Though less extensive than the GDPR, the LGPD is remarkably similar to the European inspiration, reproducing requirements on accountability, security, data minimization, purpose limitation, and privacy by design.

5.1 Territorial Scope

The LGPD will apply to any organization that stores or processes personal data about the residents in Brazil, and in a similar way to the GDPR it will operate regardless of where they are located.

5.2 Limitation of purpose, data, and storage

The data controllers and operators will only gather data within the necessary extend for the disclosed purposes and will discard personal data after the disclosed processing purpose is accomplished. Like the GDPR, those provisions carry the duty to not use personal data outside the purpose for which it was gathered; not request personal data other than necessary. It follows that the common practice of gather and keep the largest possible amount of data in order to have a record to cross reference personal information with big data analysis tools is discouraged or banned by the LGPD.

5.3 Data Security

The LGPD entails data security requirements; under the statute the controllers and operator are required to implement reasonable technical and organizational routines to ensure the protection of personal data from unauthorized access, disclosure, alteration, or destruction.

Brazil will build a body responsible for enforcing data protection, the National Data Protection Authority (ANPD), will be directly attached to the Presidency Cabinet and it is aimed to enact the regulation need to provide guidance to the minimum technical standards required.

5.4 Rights of Citizens

Following the world legislative trend, the LGPD grant data subjects a not exhaustive list of basic rights. The major rights are:

Consent: The controller must secure individual consent to be able to process and store data about Brazilian individuals and they can revoke it at any time. These consents must be specific, informed, unambiguous, and freely given.

Disclosure: the LGPD grants Brazilians rights of access, including right to correction and right to erasure.

5.5 Data Protection Officer

In a first approach, under the LGPD, every company would have to appoint a DPO, as it is required by article 41 of the statute for any and every organization that processes the personal data of Brazilian citizens. However, it expected that this provision will be attenuated by the National Data Protection Authority (ANPD) as it has powers to dismiss sectors of the economy, or companies by size or other technical criteria, as it is expected by the article 41 §3º of the statute.

An individual inside the corporation can perform the duties of the DPO, or they may be carried out by an outsourced team or even as a third-party, such as a specialist DPO service (DPO for hire).

5.6 Awareness and training

The company must create awareness among employees about LGPD requirements and are encouraged to create an environment that promotes ethical conduct, commitment to data privacy values, and compliance with the LGPD statute.

5.7 Personal data breaches

In the event of a breach, cyber-attack or accidental disclosure that could potentially infringe the privacy rights of data subjects, the company and the DPO have legal duty to notify both the national data protection authority (ANPD) and the individuals affected.

5.8 Penalties

The monetary penalties for breaking LGPD rules are relatively modest compared with other systems and, in particular with the GDPR. The maximum fine for a violation is 2% of a company's annual revenue but is capped at R$50 million (about US$9 million) per offense.

This compares with GDPR fines of up to 4% of global annual revenue or □20 million, whichever is the higher.

In comparison with the EU GDPR, it is relevant to mention that the National Data Protection Authority can create administrative requirements and directly specify the security measures that must be observed. As the industry is in rapid change the technical administrative authority will be much faster than the legislative body to accomplish that task. The GDPR, in the other hand, does not provide specific measures to be enforced in this way, however, European national enforcement agencies offer a broad guide with recommendations for security obligations.

One should note that whereas the GDPR applies strict rules to email marketing and text messaging, it is an area not directly covered by the LGPD.

As mentioned, in the GDPR model, only the public-sector organizations or private companies that store and process personal data at scale will need to appoint a data protection officer (DPO). In the other hand, as it is, the LGPD requires every company that control personal data (even their employee's data by the HR sector for instance) to appoint a DPO. But it is expected the national data protection authority (ANPD) to regulate the issue as soon as it will be operational.

6 China Data Privacy Framework

China does not yet have a federal statute dedicated to data privacy but does have a framework of regulations and laws that cover many cases. For example, the Tort Liability Law and the General Principles of Civil Law both have provisions that cover privacy and reputation as protections and that can be also applied to data. In addition to general protections, there have also been multiple specific regulations and guidelines that have been implemented or proposed.

These include: i – Decision on Strengthening Network Information Protection (2012); ii – People's Republic of China Cyber Security Law (2016); iii – National Standard of Information Security Technology – Personal Information Security Specification (last actualization in 2020); iv – Guidelines on Internet Personal Information Security Protection; v – Personal Data Protection Law (draft 2020).

The last aforementioned legislation – Personal Data Protection Law – indicates a stricter regulation than the U.S., but not as much as the EU. Until now, rather than enacting an omnibus data privacy law, China pursued a path much alike the U.S. approach, i.e., with data protection provisions comprised in laws for sectors such as banking and finance, consumer protection, postal services, healthcare, credit reporting, telecommunications, and internet, etc.

But the Personal Data Protection Law, as seen in the 2020 draft divulged in October 2021; point towards a more resembling European approach, with a larger statute encompassing the main privacy issues.

A digression is needed to analyze the Chinese Privacy Protection framework to briefly approach the context upon it has been evolving. It is paramount, prior to any data protection rule, to recognize the existence of the right to privacy in the legal system. In China, like in many countries, the idea of privacy was historically little developed or build by differently standards.

It is especially important to apprehend the structure of Chinese legal system by their own standards to avoid the bias of the orientalist or orientalism approach. The analysis by westerns benchmarks will follow requirements and criteria not necessarily consistent with local cultural, social, and legal ideals. In order to realize the real latitude of the legal protection is relevant to understand that Chinese tradition is more versed in harmony and agreements than in lawsuits and conflict. Whenever is possible to reach a solution by negotiation, mediation, and mutual compromise it will be favored by institutions even by the courts.

Another important distinction will be the emphasis on the collectivism in detriment of individualism. The interests of the group will overcome the needs of an singular agent. The occidental saying *Fiat Justitia Ruat Cælum*, a Latin legal phrase meaning let justice be done though the heavens fall, would not resonate with oriental legal systems. On the contrary it would not be welcomed by courts and society. To achieve this flexibility in civil disputes the system will prefer notions of morality and broad rules that would permit reach distinct solutions for apparently similar cases.

The privacy protection has first arisen in the geo-economic region under the Chinese influence in Taiwan and Hong Kong. Taiwan already has data protection

laws going beyond OECD standards and Hong Kong was the first jurisdiction in Asia to have enacted a comprehensive data privacy law.[11]

In Mainland, the General Principles of the Civil Law (GPCL) enacted in 1986 protect the "right to reputation" and have been employed as a basis for privacy protection. Also, the Tort Liability Law from 2010 explicitly recognizes the right of privacy along with the right of reputation and the right of honor. On March 15, 2017, the GPCL received an update providing rules for personal data protection and assessing the responsibility for breaches in data protection and collection.

In December 2012, the Standing Committee of the National People's Congress – NPC – promulgated the *Decision on Strengthening Information Protection on Networks* – "the 2012 NPC Decision" – about personal information protection in China. Then, in 2013, the NPC's Standing Committee amended the Consumer Protection Law, recognizing data protection as a right for consumers in its Article 14 and contemplating data protection principles from the 2012 NPC Decision, especially on Article 29 about security and confidentiality, purpose specification and consent.[12]

China's legal system oftentimes resorts to laws broadly drafted and somewhat flexible. In one hand, this method lacks precision gives rise to questions placing entities in a state of legal uncertainty, but in the other hand the technique offers maneuverability and flexibility to prevent the law from being outdated by evolution of technological developments.

"To complement the limitations of having vague binding laws, China uses non-binding texts to provide details and to guide the laws' implementation. In the field of personal data protection, the most important of these rules are the 2018 Specification" (Pernot-Leplay, 2020 p. 76). The Personal Information Security Specification took effect in May 2018. It places procedures for consent and how to collect, use, and share personal data.

---

11 The Personal Data (Privacy) Ordinance (Cap. 486) (PDPO) aims to protect the privacy of individuals' personal data and regulate the collection, holding, processing, or use of personal data based on a set of data protection principles (DPPs) in Hong Kong. The Ordinance came into force on 20 December 1996 but was significantly amended in 2012.

12 Consumer Protection Law art. 14: "When purchasing or using goods or receiving services, consumers enjoy the right to personal dignity, the right to have their ethnic customs respected, and enjoy the right to have their personal information protected".

Consumer Protection Law art. 29: "Proprietors collecting and using consumers' personal information shall abide by principles of legality, propriety, and necessity, explicitly stating the purposes, means and scope for collecting or using information, and obtaining the consumers' consent. Proprietors collecting or using consumers' personal information shall disclose their rules for their collection or use of this information and must not collect or use information in violation of laws, regulations, or agreements between the parties. Proprietors and their employees must keep consumers' personal information they collect strictly confidential and must not disclose, sell, or illegally provide it to others. Proprietors shall employ technical measures and other necessary measures to ensure information security, and to prevent consumers' personal information from being disclosed or lost. In situations where information has been or might be disclosed or lost, proprietors shall immediately adopt remedial measures. Proprietors must not send commercial information to consumers without their consent or upon their request of consumers, or where they have clearly refused it".

In this regard, until the Personal Data Protection Law is not fully adopted, these provisions stand out among the fragmented playing field of data privacy laws in China:

Article 25 of National Security Law of the People's Republic of China: establish network and security safeguards systems for critical information infrastructure and key sectors;[13] and, in the perspective of the cyber security, also covers network attacks, intrusion, theft as well as spreading illegal and harmful information, etc.

Article 111 of General Provisions of the Civil Law of the People's Republic of China: states the principle that natural person's personal data shall be protected by law; and, therefore, that any organization or individuals "must collect personal data after obtaining the personal data subject's consent; must ensure the security of the personal data collected; and forbids illegal collection, using, processing and transmitting of others' personal data, illegal transaction of selling or purchasing personal data, and illegal provision and disclosure of personal data".[14]

The Cybersecurity Law: articulates legal principles and operational requirements on data protection. And, finally, the 2020 *draft of the Personal Data Protection Law* PDPL that will enforce specific policies for data privacy, which are in line with global standards. This legal document is detailed below.

6.1 Territorial Scope

The draft PDPL applies to the processing of individuals' personal data that takes place in China. It will cover personal data of residents in China and eventually personal data processed in China regardless of the nationality or residence of such individuals. The draft PDPL states clear and specific extraterritorial application to overseas entities and individuals that process the personal data. It is overly broad as it covers (1) data of subjects in China for the purpose of provision of products or services; (2) analysis of behavior of data subjects in China; and (3) in other circumstances as provided by Chinese laws and regulations.

6.2 Disclosure

The draft PDPL provides the right to information and explanation on the data processing and data collecting, comprising the right to information and explanation on the data processing, right to access and request for a copy of personal data, right to correction, right to object processing, right to withdrawing consent and right

[13] LI, Lisa. A Brief Overview of China's Compliance Requirements on Personal Data Protection. *Mondaq blog*, 2020.

[14] LI, Lisa. A Brief Overview of China's Compliance Requirements on Personal Data Protection. *Mondaq blog*, 2020. Available : https://www.mondaq.com/china/data-protection/936562/a-brief-overview-of-china39s-compliance-requirements-on-personal-data-protection. Accessed: 12 Feb. 2021.

to deletion. It creates an obligation to release in the privacy notice the scope of the data that are being collected and a separate consent is required for the transfer or sharing of personal data, automatic decision-making mechanisms, etc. There is a provision for specific protocols to respond to data subjects' requests, which will further be produced by the supervising authority.

6.3 Consent

An explicit consent is due for the conclusion and performance (which are different moments in Chinese Contract Law) of a contract with individual whom data is collected. It will always be necessary for the fulfillment of statutory duties or obligations; necessary for responding to public health incidents (protection of life, health, and property); necessary for journalism or media supervision in the public interests; and, as a pattern of the provision, other circumstances as provided by Chinese laws and regulations.

The consent must be an informed, specific, freely given, indication of wishes of the data subject. And there is an explicit requirement for the need of a specific opt-in for sensitive personal data, like the ones related to race, ethnic group, religious beliefs, personal biometric data, health data, financial account data and location data.

6.4 Personal data breaches

The draft PDPL demands immediately data breach reporting and remedial measures to data breach, which are data controller's duty.

6.5 Data transfers and data tracking

Data localization requirements and rules on cross-border transfer of personal data are also envisioned; the draft PDPL proposes a data localization requirement applicable to operators of critical information infrastructure. And any cross-border data transfer is subject to security assessment to be conducted by the Chinese regulators.

6.6 Data Protection Officer

The company will designate a data protection person who will be responsible for a very comprehensive data protection compliance program to protect personal data. The PDPL, as in the 2020 draft, does not differentiate from controller to processor, and the protection officer analogue will be in charge for all the compliance and privacy enforcement.

6.7 Awareness and training

The draft PDPL demand periodically compliance audits, risk assessments, routine employee training, records of personal data processing activities.

6.8 Penalties

Violations of the draft PDPL, such as illegal processing of personal data or failure to adopt necessary measures to protect personal data, can be fined up to RMB 50 million (US$7 million) or up to 5% of the preceding year's revenue.

Also, in terms of personal liability the personnel who is personally responsible for the personal data processing may be fined up to RMB 1 million (US$ 140 thousands).

Finally, in comparison to the European GDPR is worth to register that there is some parallel to Article 82 of the GDPR and to Article 42 of the LGPD where the draft PDPL contemplates the liability of the personal data processor, unless the personal data processor can prove that it is not at fault. Therefore, there is an explicit shift of the burden of proof to the personal data processor (when comparing with the soon-to-be effective China Civil Code that provides rules on tort that can also be related to the infringement of the right to data protection).

7 Conclusions

The modern civilization migrates towards a globally digital society centered in Information. Even if that foreseen future seems distant, the modern economy already has centered itself around the data, especially personal data, as the main source of value.

Although the different statutes and regulations have similar structure and fundamental provisions the prospect of an effective personal data protection privacy system will require integration with cultural and legal social structure to meet civil rights expectations and the ability to merge with stablished core values.

Nations are struggling to adapt to the new standards and routines, aiming at a bigger integration between different organizations, under distinct jurisdictions and with diverse perspectives about civil rights, individual interests, or economic goals.

The ubiquitous spread of personal information treatment, processing and cross-referring data have highlighted the importance of privacy, data security and personal control by data subjects. The naïve movement for total transparency of corporate and governmental information has been replaced by a set of international cyber security protocols and data privacy statutes.

The full disclosure is already perceived as a utopian crusade, but the initiative to protect personal data with cryptographic protocols was embraced by the big tech

corporations. The Cypherpunk moto "Privacy for the weak, transparency for the powerful"[15] has been evolving to a complex set of national statutes and international coordination.

As explained by Professor Sarah M. Smyth:

> The process of collecting and organizing information is now a tremendous source of economic, political and cultural power. Data makes us more malleable, easier to predict, and extremely prone to influence. For retailers and marketers, being able to understand their customers' behaviors, preferences, and aversions – so they can predict their needs and provide more targeted sales pitches – is the Holy Grail.[16]

In that landscape new law is needed, and has been built, to protect the citizens' rights to privacy and to their personal information, that are being explored as commodities by data harvesting and data mining corporations. In this brave new world of information, with more personal exposition, communication speed, new opportunities and challenges the Law will be once more needed to ensure stability, justice, and concretize the expectations of the new Era.

References

ASHBEL, Amit. *Worldwide Data Privacy Regulations Compared.* Sunnyvale, CA: NetApp, Inc., 2020.

ASSANGE, Julien; APPELBAUM, Jacob; MÜLLER-MAGUHN, Andy; ZIMMERMANN, Jérémie. *Cypherpunks Freedom & the Future of the Internet*. London: OR Books, 2012.

BELL, Daniel. *The Coming of Post-Industrial Society:* a Venture in Social Forecasting. Nova York, USA: Basic Books, 1973.

BUSSCHE, Axel von dem; VOIGT, Paul. *The EU General Data Protection Regulation GDPR*. Cham, Switzerland: Springer, 2017.

FUSTER, Gloria González; JASMONTAITE, Lina. Cybersecurity Regulation in European Union: The Digital, the Critical and Fundamental Rights. *In*: CHRISTEN, Markus; GORDIJN, Bert; LOI, Michele (Org.). *The Ethics of Cybersecurity.* Cham, Switzerland: SpringerOpen, 2020. p. 97-118.

INDER, Sidhu. *The Digital Revolution:* how connected digital innovations are transforming your industry, company & career. New Jersey, USA: Pearson Education, Inc., 2016.

LI, Lisa. A Brief Overview of China's Compliance Requirements on Personal Data Protection. *Mondaq*, 2020. Available: https://www.mondaq.com/china/data-protection/936562/a-brief-overview-of-china39s-compliance-requirements-on-personal-data-protection. Accessed: 12 Feb. 2021.

MALDONADO, Viviane; BLUM, Renato. *LGPD Lei Geral de Proteção de Dados comentada*. 2. ed. São Paulo: Revista dos Tribunais, 2019.

[15] ASSANGE, Julien; APPELBAUM, Jacob; MÜLLER-MAGUHN, Andy; ZIMMERMANN, Jérémie. *Cypherpunks Freedom & the Future of the Internet*. London: OR Books, 2012. p. 141.

[16] SMYTH, Sara. The Facebook Conundrum: is it time to usher in a new era of regulation for big tech. *International Journal of Cyber Criminology,* Melbourne, 13(2), p. 578-595, jul.-dec. 2019. p. 578.

MASSENO, Manuel. Como a União Europeia procura proteger os cidadãos-consumidores em tempos de Big Data. *In*: MARTINS, Guilherme; LONGHI, João. (Org.). *Direito Digital:* direito privado e Internet. 3ª ed. Indaiatuba, SP: Foco, 2020. p. 409-428.

MAYER-SCHONBERGER, Viktor; CUKIE, Kenneth. *Big Data: A Revolution That Will Transform How We Live, Work, and Think*. London: John Murray, 2013.

MCDONALD, Aleecia; CRANOR, Lorrie. The Cost of Reading Privacy Policies. *A Journal of Law and Policy for the Information Society*, Achnabourin, Scotland. vol. 4 (3), p.543-568, 2008.

NETTER, Emmanuel. Le modèle européen de protection des données personnelles à l'heure de la gloire et des périls. *In*: NETTER Emmanuel (Org.). *Regards sur le nouveau droit des données personnelles.* Collection Colloques. Amiens, France: Centre de droit privé et de sciences criminelles d'Amiens – CEPRISCA, 2019. HAL Id: hal-02357970

NETTER, Emmanuel; NDIOR, Valère; PUYRAIMOND, Jean-Ferdinand; VERGNOLLE, Suzanne. *Regards sur le nouveau droit des données personnelles*. Amiens, France: Centre de droit privé et de sciences criminelles d'Amiens – CEPRISCA, 2019. HAL Id: hal-02357967

PERNOT-LEPLAY, Emmanuel. China's Approach on Data Privacy Law: A Third Way Between the U.S. and the EU? *Penn State Journal of Law & International Affair.* University Park, Pennsylvania: Vol. 8, (1), p. 49-117, 2020. Available at SSRN: https://ssrn.com/abstract=3542820 Accessed: 20 Mar. 2021.

SAFARI, Beata. Intangible Privacy Rights: how Europe's GDPR will set a new global standard for personal data protection. *Seton Hall Law Review,* Newark: Vol. 47(3), p. 809-848, 2017.

SARLET, Gabrielle. Notas sobre a Proteção dos Dados Pessoais na Sociedade Informacional na Perspectiva do Atual Sistema Normativo Brasileiro. *In*: LIMA Cíntia. (Org.). *Comentários à Lei Geral de Proteção de Dados*. São Paulo/SP: Almedina, 2020. p. 19-38.

SCHWAB, Klaus. *The Fourth Industrial Revolution.* New York: Random House LLC, 2017.

SMYTH, Sara. The Facebook Conundrum: is it time to usher in a new era of regulation for big tech. *International Journal of Cyber Criminology,* Melbourne, 13(2), p. 578-595, jul.-dec. 2019.

TOFFLER, Alvin. *The Third Wave*. New York, USA: Bantam Books, 1980.

TOFFLER, Alvin. *Powershift:* Knowledge, Wealth and Violence at the Edge of the 21st Century. New York, USA: Bantam Books, 1990.

TOURAINE, Alain. *La société post-industrielle*: naissance d'une société. Paris: Denoël, 1969.

WEBB, Amy. *The Big Nine*: How the Tech Titans and Their Thinking Machines Could Warp Humanity. New York, USA: Public Affairs, 2019.

ZHANG, Gil; YIN, Kate. A look at China's draft of Personal Data Protection Law. *IAPP blog,* 2020. Available at: https://iapp.org/news/a/a-look-at-chinas-draft-of-personal-data-protection-law/ Accessed: 20 Feb. 2021.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

MAGALHÃES, Marcus Abreu de. Data protection regulation: a comparative law approach. *International Journal of Digital Law*, Belo Horizonte, ano 2, n. 2, p. 33-53, maio/ago. 2021.