DOI: 10.19135/revista.consinter.00012.08

Artigos Originais

DATA PROTECTION LAW AND ITS INTERACTIONS WITH THE ANTI-MONEY LAUNDERING LAW

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E SUAS INTERAÇÕES COM A LEI DE LAVAGEM DE DINHEIRO

Adriane Garcel[1] – https://orcid.org/0000-0002-6950-6128

Sergio Fernando Moro[2] https://orcid.org/0000-0002-7449-2031

Abstract

This article aims to analyze the interactions of the new General Personal Data Protection Law, Law nº. 13,709, of August 14, 2018, with the Money Laundering Law, Law no. 9,613, of March 1998. For this purpose, the methodology used is doctrinal, jurisprudential and quantitative analysis that initially presents the principles expressly established in procedural legislation, and short definitions of their applications. Continuous action addresses the ways in which State courts, already more familiar with this interaction, react and define concepts that are still incipient in national legislation. As a result, it is concluded from the studies presented that the main interaction between the General Law on the Protection of Personal Data (LGPD) and the Money Laundering Law occurs in the institution of a central data monitoring authority at the level national. Having a critical aspect for certain doctrinal aspects, given the right to individual privacy, and as an extremely effective tool, according to divergent opinions, against modern organized crime, which implements, through detailed problems, within the privacy of certain individuals. The main contributions of this study are in the sense of evaluating the interactions that the institution of the National Data Protection Agency (ANPD) and the Money Laundering Law will carry out, especially with regard to the maintenance of a national database, and the implications this brings to the right to privacy and oblivion, in view of the prevalence of the State's interest in combating complex organized crime.

Keywords: Money laundering; Privacy; Interest of the State; Data protection.

Resumo

Este artigo visa a analisar as interações da nova Lei Geral de Proteção de Dados Pessoais, Lei nº. 13.709, de 14 de agosto de 2018, com a lei de Lavagem de Dinheiro, Lei nº.

[1] Master's student in Business Law and Citizenship at Centro Universitário de Curitiba – UNICURITIBA. Post-graduated in Applied Law by the School of the Judiciary of Paraná – EMAP and Post-graduated in Public Ministry by the Fundação Escola do Ministério Público – FEMPAR. Legal advisor to TJPR and Judicial Mediator. E-mail: adriane.garcel@tjpr.jus.br.

[2] Advisor. PhD and Master in State Law from the Federal University of Paraná – UFPR. Program of Instruction for Lawyers at Harvard Law School in July 1998. Professor in the Master's and Doctorate program at Centro Universitário de Curitiba – Unicuritiba. Title of Doctor of Laws, honoris causa, from the University of Notre Dame du Lac, South Bend, Indiana, in 2018. mestrado@unicuritiba.edu.br

9.613, de março de 1998. Para tanto, utiliza-se como metodologia a análise doutrinária, jurisprudencial e quantitativa que apresenta, inicialmente, os princípios estabelecidos de maneira expressa na legislação processual, e curtas definições de suas aplicações. Ato contínuo, aborda-se as formas que os tribunais Estados, já mais familiarizados com esta interação, reagem e definem conceitos que na legislação nacional ainda são incipientes. Como resultados, conclui-se a partir dos estudos apresentados que a principal interação existente entre a Lei Geral de Proteção de Dados Pessoais (LGPD) e a Lei de Lavagem de Dinheiro dá-se na instituição de uma autoridade central de monitoramento de dados em âmbito nacional. Tendo aspecto crítico para certas vertentes doutrinárias, visto o direito à privacidade individual, e como uma ferramenta extremamente eficaz, segundo opiniões divergentes, contra o crime organizado moderno, que se imbrica, por meio de mazelas minuciosas, dentro da privacidade de certos indivíduos. As principais contribuições deste estudo dão-se no sentido de avaliar as interações que a instituição da Agencia Nacional de Proteção de Dados (ANPD) e a Lei de Lavagem de Dinheiro realizarão, especialmente no que diz à manutenção de um banco de dados nacional, e as implicações que isto traz para o direito à privacidade e ao esquecimento[3], tendo em vista a prevalência do interesse do Estado em combater o complexo crime organizado.

Palavras-chave: Lavagem de dinheiro; Privacidade; Interesse do Estado; Proteção de dados.

Recebido/Received 30.09.2020 – Aprovado/Approved 19.01.2021

INTRODUCTION

The edition of Law No. 13,709/2018, denominated General Law for the Protection of Personal Data or LGPD, appears as a way of guaranteeing minimum protection for citizens who digitally store their data.

Among the novelties of this regulation is the incorporation of a new regulatory body in the Brazilian judicial scenario, the National Data Protection Authority (ANPD), which aims to monitor the flow of data at a national extent, as a way of ensuring greater security in the environment of the Internet.

The institution of this National Authority, considering the magnitude of the project, opens several discussions about individual privacy, which would be severely limited and opens another aspect of the discussion about the intervention of the State in private life.

Due to its recent addition to the Brazilian legal compendium, the concern is how such National Authority would act in view of the existence of other laws that would be affected by this mechanism, in particular laws dealing with crimes of a more complex typology, such as the money laundering crimes.

---

[3] In contemporary society, according to Sarlet and Ferreira Neto there is “an absolute lack of control in the handling, storage and access of personal data that are scattered on the Internet, which ends up fragmenting our sense of privacy and personality, making us vulnerable in relation to what others think and talk about our individual sphere and our past”.

The present study aims to analyze how the new General Data Protection Law affects the functionality of the Anti-Money Laundering Law.

At first, this paper will address the current legislation, Law No. 13,709/2018, having a didactical and empirical analysis whereby this Law defines its way of acting.

In a second step, it will be presented how both laws interact with each other due to the recent edition of LGPD, and how the doctrine analyzes this recent situation.

Finally, it will be demonstrated how the concepts of the General Personal Data Protection Law have been used by international courts to deal with the interactions that data protection has with the pursuit of anti-money laundering. Furthermore, it will be observed the way that Brazilian courts identify and the way that Brazilian Laws No. 13,708/2018 and No. 9,613/19 98 interact with each other and whether this interaction results in benefits or losses for the empirical application of these rules in the legal procedural system.

1 DATA PROTECTION AND ANTI-MONEY LAUNDERING

The protection of data of individuals has always been treated with extreme importance by the State, however, in view of the society integration in a cyber environment, in which almost all Internet sites require data from users, this topic has become even more central in the discussion on digital rights.

In the last few years, the number of people who have integrated with cyber systems has increased exponentially, especially with the arrival of smartphones and the invention of the wireless Internet, reaching almost 80% of the Brazilian population.4 Therefore, it is no longer possible to ignore that the lives of Brazilians, analogously to the lives of citizens of different States, orbit the cyber environment aptly named “cyberspace”[5].

In view of the progress in the digital world, the Law was pushed toward this world, however, primarily by way of tools for its convenience and functioning, such as the digital process; and the privacy protection laws were considered sufficient and only taking more importance in view of the perception of the value that the stored data of individuals could be worth[6].

Once this scenario was demonstrated, doubts arose regarding the security of user data, especially considering the long period that this type of security was still identified with the individual's privacy protection rules made prior to this period.

---

4 IBGE – Brazilian Institute of Geography and Statistics, 2018. Available at: <https://acessoainformacao.ibge.gov.br/>. Accessed on: 18 sep. 2020.

5 BENEDIKT, Michael, “Cyberspace: First Steps”, MIT Press, 1991, Available at: <https://www.academia.edu/7717050/Introduction_to_Cyberspace_First_Steps?auto=download>. Accessed on: March 12, 2020.

6 RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize, O DIREITO À PROTEÇÃO DE DADOS PESSOAIS E A PRIVACIDADE, *Revista da Faculdade de Direito* UFPR, Curitiba, PR, Brasil, v. 53, Jun. 2011, Available at: <https://revistas.ufpr.br/direito/article/view/30768>, Accessed on: April 26, 2020, doi:http://dx.doi.org/10.5380/rfdufpr.v53i0.30768.

In view of this aspect of extreme integration, certain crimes were migrated to the digital world as a way to camouflage their performance and hinder punitive action for those acts. Among those digitally perfected crimes, money laundering stands out as a complex crime outside the digital world that ends up creating paradigms for its fight.

1.1 DATA PROTECTION AND ANTI-MONEY LAUNDERING IN BRAZIL

The protection of personal data arises as the value of personal information gains importance; the market reshaped its strategies and the industries reshaped their production as of the perception of the individual 'I'.

Technological advances have also contributed to the expansion of the valorization of information collection; the advent of the computer allowed automatic data monitoring and remote information collection.

The way personal computers have revolutionized the value of user information has been impacting in a manner never seen before, initiating a discussion whether the information security parameters already adopted would be adequate to the new digital model of society. Regina Lindel Duaro and Daniel Piñero Rodriguez understand that:

> *Upon the advent of the personal computer became possible the storage and evaluation of data relating to the personal life of individuals without the need for a complex program appropriate for this purpose. Some social sectors realized how useful it could be to collect and store for later use or disclosure personal data of third parties. If until a certain historical moment the legal protection of the right to privacy proved to be sufficient, today, with the development of information technology, an unlimited number of data of all kinds is stored, which circulate between States, individuals and private companies often without any kind of control*[7].

The movement for the protection of user data gained strength and much form in the United States of America and Europe, which passed and edited specific regulations for digital data. In the United States of America, specially the existence of the Silicon Valley, is considered the main emanating source of doctrine about the surveillance of the individual and the individual freedom. In this theme Samantha Diorio explains:

> *American privacy law, on the other hand, is based primarily on the "political value of liberty from government intrusion and sovereignty within the home, rather than public image or social dignity." At its core, the American right to privacy is very much the same as it was at the founding of the nation, "the right to be free from state intrusions, especially in one's own home." American law also values the right to control access to and the distribution of personal information. The*

[7] *Idem.*

> *prime danger to Americans is that the "sanctity of (our) home (s)", using the language of a leading nineteenth-century Supreme Court ruling on privacy law, will be breached by governmental actors. There is very little concern towards the media's potential to infringe on a person's privacy, but rather the worry focuses on maintaining private autonomy within our own homes. This value is often at odds between the right of free speech and individual rights. The American law focus on individual liberty to control personal information seeks to "allow the individual to determine which information to keep private and which information to release into the public domain." However, American laws frequently prioritize free speech at the expense of individual rights. Mug shots are a prime example, as they are considered public information. This gives rise to numerous websites solely dedicated to publishing mug shots, which publicly shame those shown, regardless of their guilt or innocence, and the First Amendment protects such publication*[8].

In Brazil, the discussion on the protection of the individual in the digital environment took shape with the publication of Law No. 12,965, of April 23, 2014, better known as the Framework of Internet Law (Marco Civil da Internet). There was also the enactment of a law that deals with the protection of users' data on the Internet as a way to complement the Framework of Internet Law, Law No. 13,709, of August 14, 2018, the General Law for the Protection of Personal Data.

The General Law for the Protection of Personal Data (LGPD) in its introductory chapter lists the fundamentals for which the edition of a new regulation of the flow of cyber data is justified. Some of those principles are mainly aimed at protecting the individual's personal data, ensuring fair competition and consumer protection and freedom of expression and opinion.

The first of the protections emerged as a way of building a minimal organization for living in cyberspace. This characteristic of unrestricted freedom arises from the fact that cyberspace has no regulation at all and is inherently immune to the effectiveness of government rules[9].

This digital medium can be considered the manifestation of a theory of self-organization of digital space. Considering how people would live their digital lives, there would be an organization of rules in an autonomous way based on the social rationality of human beings.

The individual protection that the General Law for the Protection of Personal Data embraces is exactly the manifestation of the right to privacy, constitutionally

---

[8] DIORIO, Samantha, "Data Protection Laws: Quilts versus Blankets", HEINONLINE, 2015, Available at: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/sjilc42&div=15&id=&page=>. Accessed on: March 13, 2020.

[9] ORO BOFF, Salete; BORGES FORTES, Vinícius. Internet e Proteção de Dados Pessoais, uma Análise das Normas Jurídicas Brasileiras a partir das Repercussões do caso NSA vs. Edward Snowden, *Cadernos do Programa de Pós-Graduação em Direito* – PPGDir./UFRGS, Porto Alegre, v. 11, n. 1, Aug. 2016. Available at: <https://seer.ufrgs.br/ppgdir/article/view/58918>. Accesses on: March 11, 2020.

inviolable, and being the first of the guarantees to be observed in the new digital regulation, as provided in Article 2, item I of LGPD[10].

This protection is especially aimed at maintaining personal dignity and the core of their private life, bearing in mind that the damages caused by the exposure of extremely personal elements transcend the mere patrimonial damage, since the exposure will be carried out continuously by the permanence of the data and its perpetual replication in the digital environment.

It is equally correct to affirm that the individual protection expressed by this paper is the protection of the user's image. However, the Law differentiates the types of user data: personal data and sensitive data.

The first one being data that may not need the user's consent to be used in specific situations such as execution of a contract or in court, as provided in Article 7, Items III, V and VI of the General Law for the Protection of Personal Data, and for carrying out research or scientific studies, as provided in item IV of the same Article, provided that the data can be anonymized[11]. These data require in regular situations both express and tacit authorization from the user to be utilized.

The second ones are data that can be used in a harmful way towards its holder, as provided in Article 11, Paragraph 1, of the General Law for the Protection of Personal Data. Among these possibilities of harm there is, as an example of this situation, the discrimination by health plans of certain citizens for the existence of certain medical conditions, as provided in Article 11, Paragraph 5, of the General Law for the Protection of Personal Data[12].

In addition, sensitive data explicitly requires the user's consent to be utilized, so that its collection depends on the individual's will or depends on exceptional situations, such as maintaining the individual's health, compliance with legal obligation or scientific research, as long as anonymized, as provided in Article 11, Item II, 'a', 'b', 'e' and 'g' of the General Law for the Protection of Personal Data[13].

An event that redefined the paradigm of protection of individual data considered the case of exposure of the model Carolina Dieckmann, who had intimate photos exposed on the Internet in 2012.

The exposure allowed by data disclosure is unprecedented, since all digital equipment has a capacity previously unknown by Law: the ability to replicate data infinitely, with perfect accuracy and with an ability to send information extremely quick.

The Law also provides for the concept of user consent for data analysis. According to Article 5, Item XII, of the General Law for the Protection of Personal Data, it provides:

---

[10] BRASIL. Law nº 13.709, 14 august 2018. General Data Protection Law – LGPD. Brasília, DF, 2018. Available at: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>.

[11] *Id*.

[12] *Id*.

[13] BRASIL, Law nº 13.709, 14 august 2018, *op. cit*.

> *Free, informed and unambiguous expression by which the holder agrees with the treatment of his personal data for a specific purpose*[14].

The consent described by such article manifests a second aspect of the General Law for the Protection of Personal Data: the knowledge of the user's error-inducing potential, since the user's knowledge must be clearly understood not to cause an error of will.

Consent must be provided in writing, if there is a clause that defines it, and the consent resulting from knowledge of error is prohibited.

In addition, there is another aspect described in the Law that excludes from the data processing the information that the user himself has made public, as provided in Article 7, Paragraph 4, of the General Law for the Protection of Personal Data[15].

The Law establishes a situation in which data processing, whatever its type, does not require the consent of the data owner, which is the judicial investigation procedure. This topic will be discussed later.

Law No. 9,613/1998 or Anti-Money Laundering Law provides a clear need for the existence of this regulation: the blocking of insertion of criminal money in the financial system and the protection of the tax system.

The rise of the Internet is a milestone in immense technological development, however, given its extreme extraterritoriality ignoring borders and governments, a space appears without effective forms of inspection, which leaves the ideal environment for money laundering, especially with the existence of recent crypto-currencies, such as the Bitcoin, which almost eliminates the transaction of a national currency and uses a completely virtual currency, often allowing the transaction of amounts without the knowledge of the individuals who use such currency.

Based on this scenario, in-depth analysis of the General Law for the Protection of Personal Data is essential for understanding the magnitude of the Law in view of the cyber scenario. In such Law, as the new form of cyber protection, its scope ends up serving as a reference point for combating cybercrime.

1.2 LGPD: DETAILED ANALYSIS

The General Law for the Protection of Personal Data was enacted to complement the Framework of Internet Law, Law 12,965, dated April 23, 2014, and it ended up showing particular aspects and regulatory autonomy in relation to its predecessor. As a consequence, a more in-depth analysis of the new data regulation in Brazil is essential.

The new Law begins with Articles 1 to 6. In such Articles on can understand that the Law is based on the fundamental right of privacy, being effective both in the national territory and on the Internet, and interestingly it is not exclusive to digital media, affecting analog data as well, as seen in Article 1 of the General Law for the Protection of Personal Data. The National Data Protection Authority (ANDP), as provided in Article 3 of such Law, analyzes only data that has its origin in the

---

[14] *Id.*

[15] *Id.*

Brazilian Territory, which analyses is made in Brazil or the data to is used in any way in the National Territory.

Article 4 of the General Law for the Protection of Personal Data provides situations in which the justification for data collection is unnecessary, such as: the use for the preservation of the individual in matters related to health or others, the use for the execution of a judicial decision, the artistic or academic use and when the owner of the data accompanies its filtering or when the owner makes the data available for voluntarily consultation.

Article 5 of the General Law for the Protection of Personal Data provides a glossary on the more specific terms that the Law deals with and are cited later in its articles, in order to create a glossary of specific terms that would make the analysis more effective and easier to understand by the doctrine.

Article 6 of the General Law for the Protection of Personal Data, which ends the first chapter, sets out the principles of data processing. It is notable that the main purpose of this Law is to avoid the indiscriminate treatment of data as much as possible and only in situations in which data are the least harmful if they are exposed to the general public.

The 7th Article of the General Law for the Protection of Personal Data demonstrates the possibilities of situations in which data processing fits, and can be placed in three major moments: for public interest, to carry out a project, perform an obligation, conduct a research or protect the data owner, by consensual availability of the data owner and for the execution of a mandatory relationship contracted by the owner.

Articles 8 to 10 of such Law show the consequence of consent and its need. The first defines consent, which is the express manifest of the user's knowledge of data processing and his acceptance by such data monitoring method. Article 9 of the General Law for the Protection of Personal Data specifies that the data owner has unrestricted access to its data and why they are being used for in order to materialize the "principle of free access"[16]. Article 10 of the General Law for the Protection of Personal Data defines the situations in which it is checked the legitimate interest of the controller in the date processing of the user (although it does not limit to the description of such wording), the individual responsible by the processing of data treatment, and highlights that the data used will be the most necessary for the controller's purpose and that the controller must be transparent to both the user and the State when requesting information.

Articles 11 to 13 of the General Law for the Protection of Personal Data are the components of the section that treats sensitive data, that is, data that, if leaked, would cause more damage than other types of data (sexuality, health data, bank data etc.).

Article 11 of such Law defines the principles for the treatment of sensitive data, stating that they can only be used with the express approval of their owner or in the situation of research, performance of obligations or due to the need of the public administration.

Article 12 determines that data that is anonymized, data which origin cannot be traced by encryption or selective omission of details, is no longer considered

---

[16] BRASIL. Law nº 13.709, 14 august 2018, op. cit.

personal data, unless its origin is revealed, so that can be treated less bureaucratically during its use.

At the end of the section, Article 13 states that health institutions can have access to sensitive data of people due to the need to prepare a treatment or caring method for the disease or other affliction that the person may have, or even in the conception of research on new disease or additional study on an existing disease, all considering the pseudonymization of the data, that is, the data are only accessible through the existence of additional information, and the current safety parameters.

Upon entering the next section, composed only of Article 14, it is regulated the treatment of age of minors, who are absolutely or partially incapable. This extraordinary treatment follows standards of extreme protection for the child, where only specific data can be collected, only once, and must be explained didactically for both the child and the parents or guardians in order to protect the minor.

The fourth section of the General Law for the Protection of Personal Data regulates what happens to the data after the end of the treatment, consisting of Articles 15 and 16. At first, it is about the requirements for the end of the treatment, these being: legal determination, at the will of the holder, by court order or at the end of the established treatment period. At last, it shows the opportunities for storing the data after the end of the treatment, so that Article 16 provides the data maintenance as situations, as long as they are anonymized by the controller for his exclusive use, by legal determination, for transfer to third parties provided the maintenance of due caution or for future study.

The third chapter of the General Law for the Protection of Personal Data deals with the rights of the data owner, having as components of this chapter Articles 17 to 22; being the Paragraph 1 of Article 17 the fundamentals of the principle of data ownership, its non-transferability and its individuality, and the guarantee of one’s security and privacy.

Article 18 of the General Law for the Protection of Personal Data states that the data owner may request information about his data at any time from the controller, who shall be obliged to offer the data in a possible manner and within a period defined by Law or by the specific situation; in the event that it is not possible to indicate the maintainer of the data, the holder may also change, update or delete the data as he wishes.

In accordance with Article 19 of the General Law for the Protection of Personal Data, the request for information made by the data owner can be made in a written and complete or simplified manner, being the controller obliged to provide information about the data in any of these situations.

Articles 20 to 22 of the General Law for the Protection of Personal Data provide, respectively, the right to the data owner to request the review of his data, the prohibition in using the data to the detriment of the data owner and, finally, the defense of the data owners' interests can be carried out individually or collectively before the courts or by way of self-composition, according to the prevailing protection.

The fourth chapter of the General Law for the Protection of Personal Data deals with the processing of data by the Government, being composed of Articles 23 to 32.

Article 23 of such Law indicates the government as the controller of data for carrying out public policies in exceptional situations, whereby Article 26 confirms this characteristic. When the Government, through State-owned companies, acts in competition with the private sector, the Government will be treated as a legal entity under private law, as referred to in Article 24 of the same section. Article 25 of the General Law for the Protection of Personal Data allows the maintenance of a database if the implementation of public policy requires such a mechanism, respecting legal precautions.

Article 42 of the General Law for the Protection of Personal Data, states that, if confirmed, the individual responsible for the damage caused during the processing of the data must repair the damage, as determined by the Law. Article 44 of the General Law for the Protection of Personal Data explains the situations of irregularity in the treatment of data when they do not meet the basic security models, which situations are: in the manner and techniques available for the treatment of data and in the expected results and risks. Damage caused in relation to the consumer or in the jurisdiction of a special law shall follow the model of the General Law for the Protection of Personal Data as determined by Article 45.

Article 43 of the General Law for the Protection of Personal Data deals with exceptions related to the duty to indemnify in view of the damage caused. Upon proof of such situations, the exceptions that the Law provides for the data owner are: the non-performance of the assigned data processing, when the function is incompatible with the data treated, when the damage is caused by the owner himself, being caused outside the responsibility for data processing, and, finally, when the performance of the function was carried out in accordance with the Law, the damage resulting from force majeure or unpredictable circumstances.

The sixth chapter, consisting of Articles 46 to 49 of the General Law for the Protection of Personal Data, in its first section, and Articles 50 to 51, in its second section, governs security and good practices to be followed by controllers and operators of the data processing procedure.

The first section defines the basic security practices that must be followed in the event of a security breach. The article that most deals with this topic is Article 48; such article defines the parameters of minimum information that the data processing must provide in case of a data leak, these being: description of the nature of the data, information about those affected, risks involved, the security measures adopted, the reasons for delaying the actions taken if communication is not immediate and what initiatives the company has taken to deal with this situation.

Articles 46, 47 and 49 of the General Law for the Protection of Personal Data govern the same aspect that, in summary, is the adoption of security measures and those responsible for those measures. Article 46 states that companies need to take security measures to protect users' data, and some of these security protocols can be defined by ANPD itself. Article 47 defines that anyone who interacts with the data is responsible for the security of the data, even if the treatment has already ended. Article 49 states that the data processing system must be built to meet the security parameters defined by both ANPD and the company itself.

Such chapter leaves it wide open for companies to elaborate their own security standards, even though ANPD still defines the basic standards. This allows

companies to adapt to new scenarios and technologies. This is a way to follow the technological market that changes faster than the legislation can follow.

The next section is more abstract than the previous ones, as it deals with good governance practices. The most important article in this section is Article 50, which provides:

> *The controllers and operators, within the scope of their powers for the processing of personal data, individually or through associations, may formulate rules of good practices and governance that establish the conditions of organization, the operating regime, the procedures, including complaints and petitions from holders, security rules, technical standards, specific obligations for the various parties involved in the treatment, educational actions, internal mechanisms for supervising and mitigating risks and other aspects related to the processing of personal data*[17].

This article provides in its caput a very wide freedom for companies to define their administrative practices and methods of control over the functioning of their security implements. In its second paragraph it is stated that the minimum these parameters must follow encompass the company's operations, establish a relationship of trust between the company and the customer and that is adaptable in the global technological scenario.

This freedom ends up allowing a possibility that companies, in the position of workers who deal directly with the data, as they follow the course of the treatment, adapt themselves in terms of security and technology, even though ANPD encourages the edition of facilitated controls for data owners (Article 51).

The eighth chapter deals with the inspection of data processing, although such chapter also includes administrative sanctions that ANPD may take for violation of the law and exposition of users' data.

The articles of the General Law for the Protection of Personal Data dealing with sanctions are Articles 52 to 54. The main one is Article 52, which defines sanctions and the situations in which they will be applied, the main ones being: the suspension of data processing activities, or even its prohibition, publication of the leak. The application of those sanctions occurs according to the conditions of the leak and the extent of the responsibility of those involved, as reiterated in Article 54, and with the regularity of the system used in the treatment of the data. Article 53 of the General Law for the Protection of Personal Data, states that, the ANPD will treat through public consultation the methodology for calculating a fine to be applied in violation of the Law.

The last chapter of the General Law for the Protection of Personal Data deals with two bodies, the ANPD and the National Council for the Protection of Personal Data and Privacy.

ANPD, constituted under Article 55, serves as a user protection mechanism, as it is capable to sanction administratively those responsible for data security and provide guidance on the protection of users' data. Article 55 basically acts as the

---

[17] BRASIL, Law nº 13.709, 14 august 2018, *op. cit*.

cornerstone of the institution of this new agency also providing the composition and basic operational mechanisms of ANPD.

Articles 56 and 57 of the General Law for the Protection of Personal Data do not have mandatory effects due to veto effect, however, the caput of Article 55 was also vetoed.

Article 58 deals with the institution of the National Council for the Protection of Personal Data and Privacy. The first part of the article provides the composition of the Council, the second part, however, allows a glimpse of the functions of such body; the Council would be the strategic part of the virtual surveillance responsible for preparing ANPD action plans and studying the impacts of the guidelines of data protection in the population.

Article 59 of the General Law for the Protection of Personal Data has been vetoed and, therefore, will not be analyzed.

The last chapter of the General Law for the Protection of Personal Data contains supplements to this Law to be brought by later legislation. Article 60 modifies Article 7, item X, of the Framework of Internet Law which determines the exclusion of user data under the terms of the LGPD, and Article 16, item II, which enforces the exceptions described in LGPD on data considered essential to fulfill a specific purpose.

Article 61 of the General Law for the Protection of Personal Data defines that the foreign company will be notified of the procedural acts in the person of its legal representative, regardless of power of attorney or procedural act.

Article 62 of the General Law for the Protection of Personal Data provides that the National Institute for Educational Studies and Researches – INPE and ANPD will issue specific regulations on access to the database treated by the Union, in accordance with Law No. 9,934/1996 and Law No. 10,861/2004.

Article 63 of the General Law for the Protection of Personal Data governs that the ANPD will establish rules for the progressive adaptation of existing databases until the publication of LGPD. Article 64 states that the Law does not exclude other regulations that already exist on the protection of user data and its treatment.

Finally, Article 65 of the General Law for the Protection of Personal Data defines the date of entry into force of Articles 55-A to 55-L and 58-A and 58-B, and the vacatio legis for entry into force of the remaining Articles.

2 THE INTERACTION BETWEEN LGPD AND THE ANTI-MONEY LAUNDERING LAW

The main interaction that LGPD has with Law No. 9,613/1998 refers to the part where the latter defines that a register of customers and their financial transactions must be maintained, in essence, a sensitive database.

There are other interactions that exist between those laws, especially with regard to detecting the crime of money laundering. There are also critical aspects

that need to be taken into account for a better understanding of the simultaneous operation of both regulations.

In order to facilitate the interaction between both Laws, it is necessary to understand better the crime of money laundering, more specifically the empirical elements of the crime that the Anti-Money Laundering Law governs.

Money laundering consists of three phases: placement, concealment and insertion. The methods used for money laundering can be carried out and vary according to the elements available in the crime environment, so that discussing methods would be unproductive and impossible to do in this paper.

In first phase occurs the insertion of values in the national financial system. This is the most vulnerable phase, because the source is exposed for the output of the values and their initial transfer. Rogério Aro explains that:

> *This phase consists of introducing illicit money into the financial system, making it difficult to identify the origin of the values. It is the most risky phase for the "washer" due to its closeness to the illicit source. Walter Fanganiello says that it is time to "erase the stain that characterizes the illicit origin*[18].

The second phase of the offense is the concealment or sublimation phase. In this phase intermediate transactions are used in order to show a legal aspect that will increase in each new transaction and creates a false regularity of finances. Sonja Cindori explains this phase:

> *The next phase in this process is most frequently called sublimation, but it can also be called swamping or mixing (Lilley, 2000:53). In the sublimation phase, launderers start to cover traces of the real source of money by a multitude of transactions. They transfer money to domestic and foreign accounts by using legal transactions and change the shape of money in order to make it harder to follow its flow.3 In this phase the omnipresent offshore companies can be used as suitable instruments. The final goal of such money transfers is the dispersal of money and earnings and the laying of as many paper-trails as possible to confuse ongoing supervision or future investigations and finally, the making of an artificial origin or source of money*[19].

Finally, the integration phase is the final step in the money laundering process. In this phase the money is integrated into the financial system as legally obtained money. At this stage, the criminal agent receives the diverted and laundered amount and obtains the profit. Cindori also explains this phase:

---

[18] ARO, Rogerio, Lavagem de dinheiro – origem histórica, conceito, nova legislação e fases, Unisul de Fato e de Direito, *Revista jurídica da Universidade do Sul de Santa Catarina*, v. 3, n. 6, p. 167-177, jun. 2013. Available at: <http://www.portaldeperiodicos.unisul.br/index.php/U_Fato_Direito/article/view/1467>. Accessed on: April 26, 2020.

[19] CINDORI, Sonja; MURKS, Aleksandra, "The Money Laundering Prevention System, Financial Theory and Practice", 2007, p. 59-76, Available at: <https://hrcak.srce.hr/file/24818>. Accessed *on:* March 10, 2020.

> *And finally, in the phase of integration, money launderers integrate their proceeds into the economic and financial system and mix them with lawful proceeds in order to make detection of the real source of money harder (Maros, 1999:242). The final phase of the money laundering process is the integration of the illegally acquired proceeds, which have become legal and successfully embedded in the financial system. This phase is sometimes called the drying or centrifuging phase*[20].

In view of the money laundering process, it is possible to analyze the possible advances or setbacks that LGPD can cause in the interaction with the Anti-Money Laundering Law.

Starting the analysis of the possible advances or setbacks that LGPD can bring to the environment of money laundering is the constant monitoring of the environment and the behavior of individuals.

The constant monitoring of the behavior of individuals allows any anomaly in the individual's financial activity to be detected that could indicate fraud or hidden movement of illicit values.

Furthermore, the creation of a database by intermediary financial entities allows constant observation and care with the abnormal movement of values, often inserted as a cash value and later transferred to the financial system.

LGPD allows banks to be more cautious not to use or transfer this data, in order to prevent exposure of other customers, for sanctioning purposes or in order to allow more flexible control of customer information and possible money laundering suspects. In this theme of creating databases, Maria Bergström says:

> *Third, in order to enhance transparency, specific provisions on the beneficial ownership of companies have been introduced. Information about beneficial ownership will be stored in a central register accessible to competent authorities, FIUs, entities required to take CDD measures, and other persons with a legitimate interest.85 Such access to information needs to be in accordance with data protection rules and may be subject to online registration and the payment of a fee, not exceeding the administrative costs of obtaining the information.86 This section will be replaced by the fifth AML Directive, and in the future, Member States may, under conditions to be determined in national law, provide for access to additional information enabling the identification of the beneficial owner. That additional information shall include at least the date of birth or contact details in accordance with data protection rules. According to recital 14, access to accurate and up-to-date information on the beneficial owner is a key factor in tracing criminals who might otherwise hide their identity behind a corporate structure. In addition, new rules on traceability of fund transfers have been introduced*[21].

---

[20] *Id*.

[21] BERGSTRÖM, Maria, "The Many Uses of Anti-Money Laundering Regulation—Over Time and into the Future", *German Law Journal*, v. 19 n. 05, 2018, Available at: <https://www.cambridge.org/core/services/aop-cambridge-

This form of monitoring by banks allows greater flexibility in the form of monitoring financial activity as a means of preventing money laundering. Law No. 9,613/1998 provides in its Article 10:

> ***Art. 10****. The persons referred to in Article. 9th:*
>
> *I – They will identify their customers and maintain an up-to-date register, in accordance with instructions issued by the competent authorities;*
>
> *II – They will keep a record of all transactions in national or foreign currency, bonds and securities, credit securities, metals, or any asset that can be converted into cash, which exceeds the limit set by the competent authority and in accordance with the instructions issued by it;*
>
> *III – They shall adopt policies, procedures and internal controls, compatible with their size and volume of operations, which allow them to comply with the provisions of this Article and in Article. 11, in the form disciplined by the competent bodies; (Wording given by Law No. 12,683/2012);*
>
> *IV – They must register and keep their registration updated with the regulatory or supervisory body and, failing this, with the Financial Activities Control Council (COAF), in the form and conditions established by them; (Included by Law No. 12,683/2012);*
>
> *V – They shall comply with the requests formulated by COAF in the periodicity, form and conditions established by it, being responsible for preserving, under the terms of the law, the confidentiality of the information provided. (Included by Law No. 12,683/2012);*
>
> ***§ 1º*** *In the event that the client is a legal entity, the identification referred to in item I of this article shall cover the individuals authorized to represent it, as well as their owners.*
>
> ***§ 2º*** *The records and records referred to in items I and II of this article must be kept for a minimum period of five years from the closing of the account or the conclusion of the transaction, which term may be extended by the competent authority.*
>
> ***§ 3º*** *The registration referred to in item II of this article will also be carried out when the individual or legal entity, its related entities, has carried out, in the same calendar month, operations with the same person, conglomerate or group that, as a whole, exceed the limit set by the competent authority.*
>
> ***Art. 10-A****. The Central Bank will maintain a centralized registry, forming the general register of account holders and clients of financial institutions, as well as their attorneys-in-fact*[22].

---

core/content/view/B8138872E5766D59568424041195D4A8/S2071832200022987a.pdf/many_uses_of_antimoney_laundering_regulationover_time_and_into_the_future.pdf>. Accessed on: March 9, 2020.

[22] BRASIL. Law nº 13.709, 14 august 2018, *op. cit*.

The General Law for the Protection of Personal Data is a way to protect the user from the misuse of data, physical or digital, and a way to ensure greater versatility of monitoring. This interaction demonstrates a great advance for the prevention of complex crimes, as it allows the intermediary financial element to maintain a monitoring and control over the client network, which allows for a more agile detection than if it depended exclusively on special agencies of the State. It is an incredible demonstration of trust between the public and private sectors.

There are other views on this new mechanism as a way of violating the right to privacy. The institution of an authority responsible for individual's data is considered by some jurists as abusive monitoring and unnecessary monitoring, becoming a controller and limiting the individual's freedom to have privacy.

Although it does not make much sense to claim this in relation to the State, as this is the maner in which citizens obtain and register possessions and values via public notaries or banks, and the way in which the Federal Government maintains the capacity to issue essential data for civilian life.

ANPD would be a body that authorizes private institutions to maintain a database parallel to the public system, so that the private sector could be competing with the public sector in the ability to keep records on individuals and in order to control this data for profit or self-benefit.

This issue is especially relevant, mainly after Edward Snowden's case, that revealed the clandestine data collection by the United States Government. In this light, researchers Salete Oro Boff and Vinícius Borges Fortes understand that:

> *The thesis supported by Balkin (2008) and denounced by Assange (2013), evidenced in the example of use of the Deep Packet Inspection by the Chinese government gained more strength and repercussion, in June 2013, when the British newspaper The Guardian reported, with exclusivity, the first article in a series organized and signed by journalist Glenn Greenwald on the espionage programs run by the NSA – National Security Agency, the United States National Security Agency. It carried out the collection of data from telephone calls of American citizens and photos, e-mails and videoconferences of users linked to Internet services provided by American companies, such as Google, Facebook and Microsoft / Skype. Following reports, the newspaper reported to the world that the contributor to the stories was Edward Snowden, a former employee of a company that provided services to the NSA. The information delivered by Snowden made it possible to detect the existence of a secret surveillance system, called XKeyscore, which would allow US intelligence agencies to supervise routine actions common to most Internet users in the world (GREENWALD, 2013). If this revelation were not enough, in October, the Washington Post newspaper reported that the NSA had carried out a secret invasion of the connection links to the data centers of technology companies Yahoo and Google, in several countries, having access to data from a significant number of users, and also that US intelligence agencies would daily monitor the geographic location of hundreds of millions of cell phones worldwide*

> *(GELLMAN; SOLTANI, 2013). The Brazilian newspaper "O Globo" published in July 2013 an article entitled "USA spied on e-mails and calls from Brazilians", referring that Brazilian Internet users, government members, companies from key segments had been victims of the monitoring proposed by NSA programs (GREENWALD; KAZ; CASADO, 2013). The case in question is a typical example of the formation of a worldwide backlash, linked to the verification of the existence of a State of surveillance, due to the evident constitutional violation, either in the context of Brazilian constitutional law or in the North American jurisdiction. The answer to conflicts and violations of rights of this nature is usually a constitutional answer, since, in the words of Oliveira and Oliveira (2011, p. 105), "the case is due to the understanding of the Constitution, the dispute between rights in it always sheltered (expressly or implicitly), which would not lead to the most severe, drastic burden of breaking with it, that is, breaking with tradition, with constitutional history*[23].

Therefore, the main setback that this system causes is a violation of privacy through a State monitoring system or even private monitoring. The violation of privacy in defense of the security of the financial system, or even of the principles of lawful enrichment, is a demonstration of an absolute disregard for individual autonomy and the inviolability of privacy, since only the Judiciary can justifiably violate privacy to execute the legal effects of individuals' actions and the State can only violate this privacy if it is extremely essential for the execution of an action aimed at the common good or for the protection of the individual oneself.

3 FINAL CONSIDERATIONS

It is possible to conclude that the General Law for the Protection of Personal Data is a manifestation of the need to adapt Brazilian law to the new scenario of data movement in the digital sphere.

In addition, Brazilian legislation seeks to adapt to protection of user data in a more flexible way; the Law in focus allows companies to define security standards to be followed according to the need to adapt to the modern scenario.

After a more detailed analysis of the action to be performed by LGPD, a comparison was made on how it would interact with the Anti-Money Laundering Law, a current legislation that deals with a complex crime that evolved to adapt the digital elements to its execution and become an increasingly difficult crime to detect.

However, the creation of a new form of authority that serves as a form of constant monitoring of data processing ends up generating a controversy about the need for constant monitoring of citizens' activities. There is a point of view in favor and there are those who criticize the attitude of the Government and the private sector.

The defenders of this new authority, the National Authority for the Protection of Personal Data (ANPD), understand that money laundering crimes depend on

[23] ORO BOFF, Salete; BORGES FORTES, Vinícius, 2016, *op. cit*.

constant monitoring and constant care about the entry of values into the national financial market.

The monitoring system, both by the State and by individuals, would be the main way to maintain caution on the behavior of citizens as a way to detect suspicious movements of values and as a way to collect evidence about the criminal attitude of money laundering.

In opposition, critics note a violation that borders on unnecessary over-monitoring.

The right to privacy is recognized as a fundamental right; the individual has inviolable protection to one's privacy, except in extremely specific situations that deserve special care, such as protection for the person and the collective. The constant monitoring violates this punctuality and puts at risk the freedom of each one to have their privacy recognized and protected.

These being the main characteristics to be analyzed, it is possible to reach a conclusion that, in spite of the violation of freedom in view of the excessive monitoring required, the protection of the common good seems to be more necessary because it affects the collective.

LGPD mainly aims at protecting the common digital good; the protection it brings to the collective ends up surpassing the individual interest. Therefore, it is achieved the paradox of Condorcet, introduced more than two centuries ago: the sum of individual claims does not produce necessarily the best and most rational solution for the group. The legitimacy of a measure is achieved by the common good; this does not mean the simple addition of individual points of view.

REFERENCES

ARO, Rogerio, Lavagem de dinheiro – origem histórica, conceito, nova legislação e fases, Unisul de Fato e de Direito: *revista jurídica da Universidade do Sul de Santa Catarina*, v. 3, n. 6, p. 167-177, jun. 2013. Available at: <http://www.portaldeperiodicos.unisul.br/index.php/U_Fato_Direito/article/view/1467>. Accessed on: April 26, 2020.

BRANDEIS, Louis; WARREN, Samuel, The Right to Privacy. *Harvard Law Review*, v. IV, December 15, n. 5, 1980. Artigo, na sua versão eletrônica. Disponível em: <http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html>. Acesso em: 30 maio 2017.

BENEDIKT, Michael, *Cyberspace: First Steps*, *MIT Press*, 1991. Available at: <https://www.academia.edu/7717050/Introduction_to_Cyberspace_First_Steps?auto=download>. Accessed on: March 12, 2020.

Bergström, Maria, The Many Uses of Anti-Money Laundering Regulation – Over Time and into the Future", *German Law Journal*, v. 19

n. 05, 2018. Available at: <https://www.cambridge.org/core/services/aop-cambridge-core/content/view/B8138872E5766D59568424041195D4A8/S2071832200022987a.pdf/many_uses_of_antimoney_laundering_regulationover_time_and_into_the_future.pdf>. Accessed on: March 9, 2020.

BRASIL, *Law nº 13.709*, 14 august 2018, General Data Protection Law – LGPD. Brasília, DF, 2018, Available at: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>.

CINDORI, Sonja; MURKS, Aleksandra, *The Money Laundering Prevention System*, Financial Theory and Practice, 31. 2007, p. 59-76, Available at: <https://hrcak.srce.hr/file/24818>, Accessed on: March 10, 2020.

CREMER, Hans-Joachim, *Human Rights and the Protection of Privacy in Tort Law – A Comparison between English and German Law*. New York: Routledge-Cavendish, 2011.

ECO, Umberto, Quale Privacy? Disponível em: <http://www.privacy.it/archivio/eco20000928.html>. Acesso em: 17 set. 2019.

FACCHINI NETO, Eugênio, DEMOLINER, Karine Silva, Direito à Privacidade Na Era Digital – Uma Releitura Do Art. XII Da Declaração Universal Dos Direitos Humanos (Dudh) Na Sociedade Do Espetáculo, *Revista Internacional Consinter de Direito*, Estudos Contemporâneos, Publicação Oficial doConselho Internacional de Estudos Contemporâneos em Pós-Graduação, a. V, n. IX, 2º SEM., 2019, p. 119-140. Disponível em: <https://revistaconsinter.com/revistas/ano-v-numero-ix/>. Acesso em: 17 set. 2020.

DIORIO, Samantha, *Data Protection Laws*: Quilts versus Blankets, HEINONLINE, 2015, Available at: <https://heinonline.org/HOL/LandingPage?handle=hein.journals/sjilc42&div=15&id=&page=>. Accessed on: March 13, 2020.

GARCEL, Adriane, FOGAÇA, Anderson, NETTO, José Laurindo, 2020, September 10, Anti-crime law and the paradoxical affirmation of the accusatory system, *Magazine of the Faculty of Law of the FMP*, 15 (1), 8-20, Available at: <https://revistas.fmp.edu.br/index.php/FMP-Revista/article/view/170>.

GUILHERME, Gustavo Calixto; SOUZA NETTO, José Laurindo de; GARCEL, Adriane, Civil Liability for Development Risks in the Bra-

zilian Legal System, *Law and Justice Magazine*: Social and Legal Reflections, v. 20, n. 38, 2020, p. 97-113. Available in: <http://san.uri.br/revistas/index.php/direitoejustica/article/view/150>.

MORO, Sergio Fernando; GARCEL, Adriane, Dolo Eventual como Aspecto Controvérso na Lei de Lavagem ne Dinheiro, *I Encontro Virtual do CONPEDI* – Direito Penal, Criminologia, Política Criminal e Processo III, Florianópolis, 2020. Disponível em: <https://conpediql.danilolr.info/file/cc7ce59fe609bd7f353cc798dffcffd7fd72180e.pdf>.

MORO, Sergio Fernando, *Crime of money laundering*, São Paulo, Saraiva, 2010, p. 15-77 and 88-95.

ORO BOFF, Salete; BORGES FORTES, Vinícius. Internet e Proteção de Dados Pessoais: uma Análise das Normas Jurídicas Brasileiras a partir das Repercussões do caso NSA vs. Edward Snowden, Cadernos do Programa de Pós-Graduação em Direito – PPGDir./UFRGS, Porto Alegre, v. 11, n. 1, Aug. 2016. Available at: <https://seer.ufrgs.br/ppgdir/article/view/58918>. Accesses on: March 11, 2020.

RUARO, Regina Linden; RODRIGUEZ, Daniel Piñeiro; FINGER, Brunize, O Direito à proteção de dados pessoais e a privacidade, *Revista da Faculdade de Direito UFPR*, Curitiba, PR, Brasil, v. 53, Jun. 2011. Available at: <https://revistas.ufpr.br/direito/article/view/30768>. Accessed on: April 26, 2020.

SARLET, Ingo Wolfgang; FERREIRA NETO, Arthur M, *O direito ao "esquecimento" na sociedade da informação*, Porto Alegre, Livraria do Advogado, 2019, p. 20.

POSNER, Richard, Privacy, "Surveillance, and Law", *Apud* SARAT, Austin; DOUGLAS, Lawrence; UMPHREY, Martha Merrill (Ed.), *Imagining New Legalities – Privacy and its Possibilities in the 21st Century*, Stanford, Stanford Law Books, 2012.