Lisbon, 17 July 2021.

Student: Anderson Campos da Costa

Subject: Extended abstract of the Dissertation to obtain the Master's Degree and Information Security and Law in Cyberspace.

Title: THE BRAZILIAN LGPD (Law 13.709/2018), LEGAL AND TECHNOLOGICAL NODES FOR ANONYMIZATION, PSEUDONIMIZATION AND SAFE ELIMINATION OF DATA.

Advisor: Professor Carlos Caleiro

Co-advisor: Professor Raquel Castro

EXTENDED ABSTRACT

Globalization has changed the way people handle their personal data. Since the advent of the internet, social networks, online shopping and other channels, the massive disclosure of personal data is the rule.

Everything we do in our lives leaves (or will soon leave) a digital trace that can be analyzed. Recent advances in big data capture and analysis help us improve traffic congestion, accurately predict human behavior, and needs in multiple situations, and more. However, this bulk data collection can also been used against people. Simple examples of this would be charging individuals higher auto insurance premiums or refusing mortgages and jobs based on an individual's profile, as presented by the data collected. At worst, totalitarian governments to persecute, their citizens' years after data collection could use this wealth of information. Thus, the vast collection of personal data has the potential to present a serious violation of personal freedom. Individuals may face perpetual or periodically stigmatization as consequence of a specific past action, even if they have already been adequately penalized. This, in turn, threatens democracy as a whole, as it can force individuals to self-censor personal opinions and actions for fear of further retaliation.[1]

[1] Sanjam Garg, Shafi Goldwasser, Prashant Nalini Vasudevan. "Formalizing data exclusion in the context of the

This scenario changed society's conduct, with direct effects on the economy, as companies quickly needed to learn to deal with high volumes of personal data, often without due precautions regarding the protection and privacy of their holders. Therefore, we can see that the socioeconomic evolution caused the need to create legal guidelines on privacy and data protection, increasingly specific and global.

Laws must have the ability to transmit to their recipients, clearly and accurately, their rights and duties. This is not always the case and it is not uncommon to find people lost in the complexity of the legislative web.[2]

In this context, in August 2018, in the Brazilian state, the Brazilian General Data Protection Law (Law No. 13,709/2018) entered into force, or only LGPD as it will been referred to in this work. The LGPD has imposed a wide list of rights for data subjects and obligations for companies controlling personal data. However, the legal text did not address the way of performing the procedures necessary for its purpose, that is, it left it up to the data controller to decide which methods and techniques anonymization, pseudonymization and deletion of data should adopt for the attendance of the LGPD.

In this perspective, the present work will address the legal foundations and objectives, then, from the technological perspective, the functionalities and applicability of anonymization methods and techniques, pseudonymization with special focus on the safe elimination of data with the generation of auditable evidence will been treated.

HISTORIC

The right to privacy has a parallel to the very history of civilization, because it is something related to the intimate, the private. In this respect, the *Global Internet Liberty Campaign website* supports understanding[3] that:

> Privacy has deep roots in history. The Bible has numerous references to privacy. There was also a real protection of privacy in the early days of Hebrew, Classical Greek and Chinese cultures. Most of these protections focused on the right to been left alone.

right to be forgotten." EUROCRYPT (2) 2020: 373-402.

[2] MATIAS MAGALHÃES, Filipa; LEITÃO PEREIRA, Maria. General Data Protection Regulation, Practical Manual (2nd Revised and expanded Edition), Porto: Vida Económica, 2018. p.78

[3] GLOBAL INTERNET LIBERTY CAMPAIGN. PRIVACY AND HUMAN RIGHTS: ***An International Survey of Privacy Laws and Practice***. Available in: <http://gilc.org/privacy/survey/intro.html>. Access: 20 Jul. 2020.

Thus, in view of the socioeconomic changes brought about by the industrial revolution, the obligation arose to protect the right to privacy against interference from other people, whose milestone was made through the UN Universal Declaration of Human Rights in 1948, which brought in article XII the provision of the right in question.[4]

From this, the need to create legal guidelines on the protection of increasingly specific and global data has been established. In Bauman's view, the current modern scenario requires this "mass surveillance", that of the right over all individuals. According to the author:

> In the current scenario of modernity, the separation between politics and law remains a point of reflection and design of the debate. While power has become a global and extraterritorial phenomenon, with the proliferation of centers of power beyond state relations, politics has been drastically reduced to a local phenomenon – with significant repercussions in global villages – unable to react, both in the public and private spheres, and provide mechanisms of political control to the uncertainties and technological advances of modernity. In a scenario of global villages with their own regulatory networks, more than ever the role of politics has become essential to provide structural coupling between state and private activity to avoid the lack of interoperability between privacy and data protection regulations.[5]

Thus, one of the most disturbing aspects in the analysis of data protection and privacy involves the delimitation of the appropriate concept to protect the individual sphere.

In the 1960s, under the leadership of the United States and some European countries, large-scale, centralized data processing projects emerged.

In the 1970s, survey censuses emerged in the United States, which began to collect data on private housing in society. With this, the search for information about the intimate minutiae and the private life of citizens came along, which resulted in the citation:

> The hypothesis that explains why this growing form of invasion is the fact that it simply became feasible, for the technology of the time, to process this information and extract some utility from it – and what was new was not the

[4] Article XII - No one shall be subjected to interference in your private life, your family, home or correspondence, or attacks on your honor and reputation. Everyone has the right to protection of the law against such interference or attacks.
[5] BAUMAN, Zygmunt. **Net surveillance:** dialogues with David Lyon. Trad. Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013. p. 13.

utility, but the fact that its obtaining was made possible.[6]

As early as 1981, a convention bringing together the member countries of the Council of Europe called for the unified and expanding standards for the automated treatment of personal data[7].

The design of the European Economic Community - EEC - has boosted the indigence of one legislation for data processing. However, the European Union's regulatory processes – which are adept at the denomination thanks to the Maastricht Treaty in 1992 – take into account the legal dissimilarity of its components. [8]

In 1995, the first unified European legislation emerged Directive 95/46/EC, which had the protection of individuals in the processing of their personal data and the movement of them within the European Union.

In the United States, where there is great recourse to self-regulatory and where the state seeks to interfere, creating norms, only in areas considered sensitive, such as health, finance and minors. In this model, although there is some tendency to judicialization, the focus is freedom of contracting and the possibility of the market defining, in its interaction with consumers, acceptable behaviors. [9]

Currently, the European and American model are references for the structuring of data protection standards in world democracies.

RIGHT TO PRIVACY AND INFORMATIONAL SELF-DETERMINATION

The right to privacy, in its initial formulation, was been related to the protection of the intimate, family and personal life of individuals. The right to Information All Self-Determination, which is been understood as the "right of each individual to control and protect his/her own personal data, in view of modern technology and information processing". Also called the right to informational and decisional privacy by some scholars, because it is a subspecies of the right to privacy genre. [10]

In sum, good constitutional doctrine considers as the existence of a "general right

---

[6] DONEDA, Danilo. **From privacy to the protection of personal data.** Rio de Janeiro: Renova, 2006, p. 9-10.
[7] Ibidem.
[8] VIDOR, Daniel MARTINS, **LGPD: origin and implications**. Available in: <http://mercurylbc.com/lgpd-origem-e-implicacoes/>. Access: 8 Sep. 2020.
[9]Guidi, Guilherme Berti de Campos. **REGULATORY MODELS FOR THE PROTECTION OF PERSONAL**DATA; Available in: https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf. Access: 17 Jul. 2021.
[10] MARTINS, Leonardo (Org.). **Fifty years of jurisprudence of the German Federal Constitutional Court. Montevideo : Konrad** Adenauer Foundation, 2005, p. 233-235.

to informative self-determination that translates, fundamentally, into the faculty of the individual to determine and control the use of his data".[11]

It is worth saying that this right was been first brought to light by the German Constitutional Court in the judgment of the German Census Law of 1982. According to this Court, the right to informational self-determination "presupposes that, even under the conditions of modern information processing technology (...), that the individual exercises his freedom of decision on the actions to be preceded or omitted in relation to his data".[12]

Therefore, the right to informational self-determination emerges as a dismemberment of the right to privacy, with the purpose of effectively protecting the set of data considered personal of citizens, guaranteeing them control over them.

THE BRAZILIAN GENERAL DATA PROTECTION LAW

Influenced by the principles of the European GDPR, the General Data Protection Law (Law No. 13,709/2018) emerged. Right at No. Article 4(1) of the GDPR, "personal data" has been defined as information relating to an identified or identifiable natural person of the "data subject", and an identifiable natural person is considered to be an identifiable natural person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, identification number, location data, electronic identifiers or to one or more elements of the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[13]

The Brazilian LGPD, is situated as a means of effective personality rights, through principles and rules, establishing national regulation on the processing of data, in order to avoid distortions in the processing of information considered personal data.[14]

The law indicates principles that should govern data processing activities, such as good faith (objective), purpose, adequacy, transparency, among others. It is required, in a sense, which the processing of data be are carried out from purposes compatible with the legal order, that the data collected be used only in these purposes and that the

---

[11] CANOTILHO, JJ Gomes. **Constitutional Law and Theory of the Constitution.** Coimbra. Ed. Almedina, 2003. p. 20.
[12]VIEIRA, Tatiana Malta. **The right to privacy in the information society: effectiveness of this fundamental right in the face of advances in information technology.** Brasilia, 2007. 296 ps. Dissertation (Master's degree in Law, State and Society). University of Brasilia, Brasília, 2007. p. 88.
[13] **GDPR**. Available in: <https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679#d1e2479-1-1>. Accessed 5 Feb 2021.
[14]COELHO, A.C.B. **The Brazilian General Law for the Protection of Personal Data as a means of effective personality rights.** João Pessoa: [s.n.], 2019. p. 55.

processing take place in a careful and crystalline manner, providing ample shelter to the human person.[15]

In 2019, Law No. 13,853/2019 is been enacted, which included Articles 55-A and the following into the LGPD, creating the National Data Protection Authority (ANPD). In this respect, intelligence of Paragraphs 1 and 2 of Article 55a, shallbe:

> [...] this nature appears to be transitory, and the Authority may be transformed by the Executive Branch into an entity of the indirect federal public administration, subject to special municipal regime and linked to the Presidency of the Republic, and such transformation must be evaluated within two years of the date of entry into force of the regimental structure of the ANPD.[16]

The note is necessary to the extent that the experience of other countries shows that the total independence of the Supervisory Authority in relation to the executive branch becomes indispensable, because the Public Power invariably is a violator of the privacy of individuals.

Despite the great influence of the European GDPR on the LGPD, the Brazilian legislature did not take care of criminal aspects related to bad practices involving personal data.

Therefore, 26/11/2019, was been instituted by Act of the President of the House of Representatives, a Committee of Jurists with the objective of drafting the Draft Data Protection Law for public security and criminal investigation. After one (1) year, the President of the Chamber of Deputies was been handed over to the Draft of the Data Protection Act dealing with criminal matters.

It is still premature to say how or when the Draft Will evolve into a Bill, but the first step towards criminalizing conducts against the protection of personal data has been taken. Considering the speed of events on the internet with increasing impacts in the legal and socioeconomic sphere, it would not be pessimistic to believe that its enactment will not take long.

PRIVACY AND DATA PROTECTION

The concept of data can been defined as "a set of records about facts, which can be ordered, analyzed and studied to reach conclusions". These data, when "organized

[15]Ibidem.
[16]SCHREIBER, Anderson. **Manual of civil law:** 3. ed. São Paulo: Saraiva Educação, 2020. p. 209.

and ordered in a coherent and meaningful manner for the purpose of understanding and analysis", are been called Information. [17] And when you add the word "personal" to the term "data", there is a customization of the concept, so that "personal data" would be a set of records referring to an individual.[18]

The fundamental premise for privacy and data protection to be effective and *sine qua non* that, the data controller in the figure of the EPD is absolutely honest and faithful to its obligations, that is, only professionals interested in fully complying with the legislation are able to benefit from the suggested model. Because in this scenario, the main opponents can be the tutors themselves.

Thus, the premises of honesty and professionalism should permeate all information security processes, fundamentally those related to the protection of personal data established by the LGPD. It happens that, the legislation does not specifically indicate, how data processing to be done.

PSEUDONYMIZATION

In Brazil, the definition of pseudonymization is described in Article 13, § 4 of the General Data Protection Law:

> For the purposes of this article, pseudonymization is the treatment by which a data loses the possibility of association, directly or indirectly, with an individual, but by the use of additional information maintained separately by the controller in a controlled and safe environment. [19]

As for use, the application of pseudonymization for the protection of personal data in the GDPR has a wide applicability, while in Brazil it is been only used for the processing of sensitive personal data, in accordance with article 11 of the LGPD.

The interpretation of pseudonymization as an extra safety measure was adopted *by Working Party 29 in Opinion on Anonymisation Techniques*[20] when Data *Protection*

---

[17] LACOMBE, Francisco José Masset et al. **Administration - principles and trends**. São Paulo: Saraiva, 2003. p. 490.

[18]TAVARES, Letícia Antunes; Alvarez, Bruna Acosta**(The protection of personal data: a comparative analysis of the regulatory models of Europe, the United States of America and Brazil.** Available from: <http://www.tjsp.jus.br/download/EPM/Publicacoes/ObrasJuridicas/ii%204.pdf?d=636680444556135606>. Access: 7 Sep. 2020.

[19] Brazil. **General Data Protection Act, Law**13,709 of 2018. Available in: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Access: 8 Sep. 2020.

[20]UNITED KINGDOM. ***Information Commissioner's Office. Anonymisation:*** *Managing Data Protection Risk Code of Practice.* 2012. p. 22. Available in: <https://bit.ly/2qwK1xy>. Access on 13 Sep. 2020.

Directive 95/46 was in place. The *GDPR* mentions in Article 25 that pseudonymization is a way of effecting the principle of privacy by *design.*

Ultimately, in pseudonymization there are no specific legal advantages in the LGPD, apart from being considered a technique for improving information security.

Entering the technological area the pseudonymization process consists of replacing identifying data with invented data, this technique can be called encoding.

The pseudonymization process, even if it has ensured the highest levels of security, there will always be a risk of reidentification of the data subject. Therefore, contrary to anonymized data, pseudonymized data are still within the scope of the GDPR, since there is a substantial risk of re-identification of data subjects. Being the same scenario applied to LGPD. [21]

As a rule, pseudonymization should been applied concurrently with other anonymization techniques, because when used alone, pseudonymization will not result in an anonymous dataset, that is, the data holder will probably be identified indirectly, so the process can be reversed.[22]

The large amount of personal data made available by the data subject himself, through the internet, can facilitate the attack. Even in isolation, this data may seem anonymous, but by combining this data with other sources, you can eventually re-identify the data subject.

A dataset can suffer from various types of reidentification attack. Currently there is a lot of research that aims to demonstrate how a set of data can be re-identified, for example public data entered in social networks, dissemination of data from demographic studies, data from genome sequence studies, information on mobility patterns, film evaluations and even people's writing style can be used for reidentification

[21] SEQUEIRA, C.S.A. "Digital Identity – The Spectrum from Anonymization to Identification," Master's thesis, Instituto Superior Técnico, 2019.

[22]"Opinion 05/2014 on Anonymisation Techniques". Article 29 Data Protection Working Party(European Commission) on 10July2014. Available in: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf. Accessed: 10 Aug. 2020.

attacks.[23][24][25][26][27][28]

Many of these attacks use data disclosed by their own owner on their social networks such as: the address; gender; attribution of authorship, among others. In a data set one can find several levels of the risk of reidentification, because the more information the user discloses on their social networks, the greater the risk of reidentification. Thus, the greater the effectiveness of the application of anonymization techniques, the lower the risk of reidentification of the data subject. [29][30][31]

However, the increase in safety has a negative impact on the practical usefulness of the data, because the higher the anonymization, the lower the unidentifyability.[32]

ANONYMIZATION

Article 5 of the LGPD(III) contains a definition of "anonymised data", and any "data relating to a holder that cannot be identified, considering the use of reasonable technical means available at the time of its treatment". [33]

Also, in the same article, in item XI, one has the meaning of the process that transforms information into a given anonymized: anonymization. Being is the "use of reasonable technical means available at the time of treatment, through which a data

---

[23] D. J. Crandall, L. Backstrom, D. Cosley, S. Suri, D. Huttenlocher, and J. Kleinberg, "Inferring social ties from geographic coincidences," Proceedings of the National Academy of Sciences, vol. 107, no. 52, pp.22 436–22 441, 2010.

[24] P. Golle, "Revisiting the uniqueness of simple demographics in the us population," in Proceedings of the 5th ACM Workshop on Privacy in Electronic Society, 2006, pp. 77–80.

[25] GYMREK M [et al.] - Identifying personal genomes by surname inference. In: Science.
HOMER, Nils [et al.] - Resolving individuals contributing trace amounts of DNA to highly complex mixtures using highdensity SNP genotyping microarrays. In: Genet PLoS.

[26] DE MONTJOYE [et al.] -Unique in the Crowd: The privacy bounds of human mobility. In fashion. Sci Rep.
GAMBS, Sébastien; KILLIJIAN, Marc-Olivier; NÚÑEZ DEL PRADO CORTEZ, Miguel - De-anonymization attack on geolocated data. In: Journal of Computer and System Science.

[27] NARAYANAN, Arvind; SHMATIKOV, Vitaly - Robust De-anonymization of Large Datasets. In: SP '08 Proceedings of the 2008 IEEE Symposium on Security and Privacy.

[28] NARAYANAN, Arvind [et al.] - On the feasibility of internet-scale author identification. In: Proceedings of 33rd IEEE Symposium on Security and Privacy.
MARKOV, Ilia; BAPTISTA, Jorge; PICHARDO-LAGUNAS, Obdulia - Authorship Attribution in Portuguese Using Character N-grams. In: Acta Polytechnica Hungarica.

[29] ELMONGUI, Hicham G.; MORSY, Hader; MANSOUR, Riham - Inference models for Twitter user's home location prediction. 2015 IEEE/ACS 12th International Conference of Computer Systems and Applications (AICCSA).

[30] DEITRICK, William [et al.] - Gender Identification on Twitter Using the Modified Balanced Winnow, In: Communications and Network;
BURGER, John [et al.] - Discriminating gender on Twitter. In: Proceedings of the Conference on Empirical Methods in Natural Language Processing (EMNLP '11).

[31] YAN, Jinny; MATTHEWS, Suzanne - Applying clustering algorithms to determine authorship of chinese twitter messages, In: IEEE MIT Undergraduate Research Technology Conference (URTC).
ALMISHARI Mishari [et al.] - Stylometric linkability of Tweets. In: Proceedings of 13th Workshop on Privacy in the Electronic Society.

[32] Of unidentifiable, according to the dictionary is what can not be identified, in Online Dictionary of Portuguese, https://www.dicio.com.br/inidentificavel/ [consulted on 16-02-2021].

[33] Complete wording of Article 5, item III, of the LGPD: For the purposes of this Law, it is considered: III - anonymized data: data relating to the holder who cannot be identified, considering the use of reasonable technical means and available at the time of its treatment.

loses the possibility of association, directly or indirectly, with an individual".[34]

According to the understanding of Thiago Luis dos Santos Sombra, in order to achieve anonymization, it is necessary that personal data have been collected and processed in accordance with the rules of the category, since if the process has any bias, the controller will answer for the period in which the data were able to be associated with an identifiable person. [35]

In this way, it is permissible to interpret the reading of the new regulations, which will be necessary for those involved to use techniques to make anonymization possible. However, the law does not inform how this should been done.

In the technological area, the process of anonymization of data has the function of protecting the identity of the individual, even when the data is disclosed to the public, preventing the association of a given with a given person.

There are different anonymization techniques, each with specific characteristics and applicability, the main ones[36] being: Anatomization, Generalization, Suppression, Permutation, Disruption, Synthetic Data and Data Aggregation.

Before use, analysis are recommended and align the technique in relation to the existing scenario and the desired objective, because the isolated application or set of techniques should ensure the complete anonymization of the data, that is, the impossibility of identifying the data subject, the process will be aligned with the LGPD.

Finally, you should point out that the whole procedure must be auditable and the documentation remains available to the supervisory entities.

DATA ERASURE AND ENCRYPTION

In order to provide individuals with more control over their own information, the LGPD regulated a concept already provided for in the Marco Civil da Internet, “the right to erase data”.

The right to erasure of data appears in Article 18 of the General Data Protection Law, which establishes that the data subject may request the controller, at any time and upon request, among others: access to the data processed by the controller; correction

[34] XI - anonymization: use of reasonable technical means available at the time of treatment, through which a data loses the possibility of association, directly or indirectly, with an individual.
[35] I'm going to go. p. 171.
[36] ditto

of incomplete, inaccurate or outdated data; anonymisation, blocking or deletion of unnecessary, excessive or lgpd non-compliant data; data portability to another service or product provider; withdrawal of consent; deletion of personal data processed with the consent of the holder.[37]

The legal provision that data subjects have the right to see them safely deleted has been enshrined in the LGPD. However, the legislator did not determine how to eliminate the data.

In this sense, two big questions arise: first, how the controller proves the deletion of data; second how the inspection bodies check the effectiveness of the data elimination process.

Traditional methods of overwriting elimination used in magnetic media are not effective in more modern data storage systems. In this way, the removal of files on disk is a problem when you want to be permanently erase the data.[38]

Authors Feng Hao, Dylan Clarke and Avelino Francisco Zorzo in the article "Deleting Secret Data with Public Verifiability" described a cryptographic solution with the aim of making the data erasure more transparent and verifiable.[39]

This encryption method causes each block written to the disk to be encrypted by a distinct key, and when a block must be deleted simply deletes the key, that is, the problem of safe deletion of a file is replaced by the problem of safe deletion of a cryptographic key. Using this, technique it is no longer necessary to delete large amounts of data, but rather to delete a key from 128 to 256 bits. [40]

Since the main objective is to carry out a safe elimination, the generation of keys is automatic, through random numbers in the protection system that also manages for the controller.

Back to using encryption for data erasure, if the math behind encryption is good, process reversibility is impossible is unlikely.

For example, it is unlikely that a 256-bit symmetric key (with solid mathematics) will be broken anytime soon. How is this statement still true in today's world of millions

[37]BRASIL. **General Data Protection Act, Law 13,709 of 2018.** Available in: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm>. Access: 8 Sep. 2020.
[38] Joel, R.; Srdjan, C., Basin, D. "Data Node Encrypted File System: Efficient Secure Deletion for Flash Memory." In: Proceedings of the 21st USENIX Conference on Security Symposium, USENIX Association, 2012, pp. 17–17.
[39] Hao, F.; Clarke, D.; Zorzo, A. F. "Deleting Secret Data with Public Verifiability." IEEE Transactions on Dependable and Secure Computing, vol. 13 (6), 2016, pp. 617–29.
[40] Hao, F.; Clarke, D.; Zorzo, A. F. "Deleting Secret Data with Public Verifiability." IEEE Transactions on Dependable and Secure Computing, vol. 13 (6), 2016, pp. 617–29.

of cloud-based computers and faster graphics processor units (GPUs)? Can't attackers try to guess all the possible combinations resulting from 256 0 and 1 different? The answer is no, due to the large number of possible keys that can be formulated from all combinations of 256-bit keys.[41]

The computers in the world do not have enough memory or hard drive space to store everything that would been needed to break a decent encryption key. If you could somehow create and connect a billion computers, each making 2 billion guesses per second, it would still take longer than the estimated age of computers in the universe (for example, 14 billion years). In addition, there is not enough energy in the universe to actually perform the break.[42]

The process of erasing personal data through random key generators and encryption techniques with homomorphic properties, presents advantages with regard to end-to-end security of the process, which are the bases for carrying out the procedures of audit and inspection, as it ensures the irreversibility of the process attending art. 5th, 14th of the LGPD.[43]

The generation of evidence of data elimination supports analytical and synthetic certification, obtained through the analysis of metadata and the execution of search algorithms in the encrypted file, fulfilling Art.19 of the LGPD.

Therefore, and this work presents precise general understandings of what is required of an honest data controller to faithfully meet the legal commands of the LGPD, at least intuitively when mirrored in the legal understandings already pacified in the European GDPR.

It still offers technically accurate definitions for data erasure, which represent possibilities for interpretations of what legislation could reasonably expect, in addition to alternatives to what future versions of the law could explicitly require.

KEYWORDS: Brazilian General Data Protection Law (Law No. 13,709/2018); Right to Privacy and Right to Informational Self-Determination; methods and techniques of anonymization, pseudonymization, data deletion, cryptography and homomorphic.

[41] "What is encryption payment? Available in: https://www.blancco.com/resources/article-what-is-cryptograhic-erasure. Access on 03/08/2020.
[42] I'm going to go.
[43] Art. 5 º For the purposes of this Law, it is considered:
XIV - deletion: deletion of data or data set stored in a database, regardless of the procedure employed;