RCMOS – Multidisciplinary Scientific Journal O Saber.
ISSN: 2675-9128. Sao Paulo-SP.

OPEN BANKING: EVOLUTION OR VIOLATION OF LGPD

OPEN BANKING: EVOLUTION OR VIOLATION OF THE LGPD

Jonathas Alves Mesquita[45]
José Elias Seibert Santana Junior[46]
Submitted on: 05/16/2022
Approved on: 05/16/2022
Published on: 05/16/2022 v. 2, no. 1, Jan-Jun. 2022
DOI: 10.51473/rcmos.v2i1.295

SUMMARY
This article sought to present Open Banking and the General Data Protection Law (LGPD). Open Banking is a system that allows the bank to share its customers' information in order to suggest improvements and different plans for them. Therefore, this study had the general objective of discussing the evolution or violation of the LGPD within the scope of Open Banking. The methodology used was a literature review, where different databases (national and international) were consulted in order to analyze the scientific documents available on this topic, collecting information and compiling it. Therefore, the importance of authorizing or not authorizing the Bank to share the data is concluded in order to protect personal information.

Key words: Open Banking. General Data Protection Law. LGPD.

ABSTRACT
This article sought to present about Open Banking and the General Data Protection Law (LGPD). Open Banking is a system that allows the bank to share its customers' information to suggest improvements and different plans for the same. Thus, this study aimed to discuss the evolution or violation of LGPD in the context of Open Banking. The methodology used was the literature review, where different databases (national and international) were consulted to analyze the scientific documents available on this subject, collecting information and compiling them. Thus, it is concluded the importance of authorizing or not the Bank to share data, to protect personal information.
Keywords: Open Banking. General Data Protection Act. GDPR

1. INTRODUCTION

This study sought to develop the theme “Open Banking: Evolution or Violation of the LGPD”. With technology evolving more and more and banking procedures being digitized, the General Data Protection Law (LGPD) states that any information regarding the customer must be kept confidential unless the customer requests that their data be shared.

As a hypothesis we will have:

a) The bank must keep customer data in absolute secrecy and not share it;
b) When hiring a bank, the customer must be aware of the data preservation policy;
c) The client must disclose to their manager that their data remains strictly confidential and can only be shared with prior authorization.

This study presented the following problem: How did the LGPD evolve or violate open banking?

By general objective we have: Discuss the evolution or violation of the LGPD within the scope of Open Banking and by specific objectives: a) Conceptualize the LGPD (General Data Protection Law); b) Discuss open banking: its features, benefits, applications and c) Explain how the LGPD evolved or violated open banking.

With increasingly frequent access to the internet, banks have modernized and with this, open banking has emerged, which must be in accordance with the LGPD in order to guarantee the security of its users.

Thus, this study is justified by bringing important implications for society and scholars in the area, also serving as academic support for future research.

2 METHODOLOGY

45
46 [1]Graduating in Law from Faculdade Santo Agostinho – FASAVIC (STUDENT)
Attorney. Professor of Labor Law, currently coordinator of the Law course at FASAVIC.
Specialist in Labor Law and Labor Procedural Law from Damásio de Jesus College. (ADVISOR)

For this study to be developed, the descriptive method will be adopted, with a qualitative approach. Shank (2002 p. 5) defines qualitative research as “a form of systematic empirical investigation into meaning”.
By systematic, he means “planned, orderly, and public,” following rules agreed upon by members of the qualitative research community. By empirical, he means that this type of investigation is grounded in the world of experience.

Inquiry into meaning says that researchers try to understand how others make sense of their experience. Denzin and Lincoln (2000 p. 3) state that qualitative research involves an interpretive and naturalistic approach: “This means that qualitative researchers study things in their natural environments, trying to understand or interpret phenomena in terms of the meanings that people bring to them. they".
The study was prepared through literature review research. For Marconi and Lakatos (2010), a literature review is a critical analysis of published sources, or literature, on a specific topic.
It is an assessment of the literature and provides a summary, classification, comparison and evaluation. At the graduate level, literature reviews may be incorporated into an article, a research report, or a thesis.
At the undergraduate level, literature reviews can be a separate stand-alone assessment.
For Köche (2011), the literature review is generally in the format of a standard essay composed of three components: an introduction, a body and a conclusion. It is not a list like an annotated bibliography in which a summary of each source is listed one by one.
The search will be carried out in databases of Latin American and Caribbean Literature in Health Sciences (LILACS), Scientific Electronic Library Online (SCIELO), monographs, dissertations, scientific articles.
The inclusion criteria for the bibliographic survey of this study will be text available in full for free, in Portuguese and English and that meet the proposed objectives. Exclusion criteria will be studies that do not meet the study objectives.

3 OPEN BANKING CONCEPT

The customer owns their data, not the bank. This is the proposal of Open Bank, which is responsible for making the user the protagonist of control and allowing financial institutions to access their personal information. The open banking model aims to expand the offering of banking products and services at a lower cost. However, the big challenge will be to create appropriate methods to collect and manage consent for the processing of personal data (GOETTENAUER, 2020).
Open banking is a way to expand banking products and services at a lower cost, creating healthier competition between banks and financial technology. However, in this case, taking into account the General Data Protection Law (LGPD), the biggest challenge will be to create an adequate process to collect and manage the customer's consent to participate in this new model and the processing of personal data (BARBERIS; BUCKLEY; ARNER, 2015).
In the model stipulated by the Central Bank, financial institutions are classified as S1, which is equal to or greater than 10% of the Gross Domestic Product (GDP) or financial institutions with related international activities, and S2, which has a scale between the two of the institutions Participating in an open bank require 1% and 10% of GDP (BARBERIS; BUCKLEY; ARNER, 2015).
Therefore, as long as customers authorize data sharing, large banks operating in Brazil will be obliged to participate. On the other hand, other institutions, such as payment companies and fintech companies, will have voluntary participation and must share customer data with competitors (MAGNUSON, 2017).
This situation leads to the basic approach of open banking: reciprocity, taking into account that all participating companies have the right to receive data from competitors and are obliged to share it, as long as the customer agrees. Thus, free competition expands and benefits those most interested, namely consumers, who will have the option of sharing data, which will be digital and conducted in a safe environment and supervised by Central Bank regulators. The process will comply with the General Data Protection Law (LGPD) and will follow a standard process agreed by customers, similar to accessing institutions through applications or online banking through facial recognition, biometrics or passwords (VIOLA; HERINGER, 2020).

As Open Banking is based on consent, which is one of the legal foundations of the LGPD, customers can authorize or revoke sharing at any time. It is worth noting that this acceptance is specific, that is, customers only allow certain data to be shared with third-party banks, and it is not universally applicable to all data or all institutions.
The internet or network is known as the most powerful means of communication in the world, it is capable of connecting us to any desired information in about an instant. However, the Internet as we know it today was designed for military communications in the 1960s, when an information sharing system was created to facilitate war strategy.

Thus, the initial milestone of the Internet was called ARPANET, a system in which information was broken into small packets containing pieces of data and, in the event of an attack, it was difficult for an adversary to obtain all the desired information. It was not until the 1990s that the famous "Internet boom" emerged, with the advent of the www (World Wide Web) and other browsers, popularizing the use of the Internet as a global network of connected computers.

It is no different in Brazil, where the internet took its first steps in the 90s and stabilized as a form of communication in the 2000s. With the development of the Internet, forms of search expanded, information became more accessible to users, The Internet has become a true ally in the dissemination of information, the convenience of technology has brought reconfiguration, that is, a way of distributing information and data has been created. Thus, it is confirmed that new questions have arisen about privacy and ease of movement of personal data, and the need for protection has become clearer. In 2014, Brazil passed a law regulating Internet discipline, the Marco Civil da Internet, to keep Internet users safe.

However, this new law does not guarantee data privacy in a complete, comprehensive and structured way, and is not a general data protection provision, concluding that the protection of personal data remains unprotected and legislation is needed that guarantees respect for privacy . Community flow of personal data.

The LGPD (General Data Protection Law) is defined in Law 13,709/18, which provides for the processing of personal data, including digital media, by natural or legal persons governed by public or private law for the protection of freedom and fundamental rights. privacy and the free development of the personality of individuals (BRASIL, 2018).

4GENERAL DATA PROTECTION LAW (LGPD) AND ITS PARTICULARS

In Wheaton v. Peters, 1834, but was not officially known until 1890, Louis Brandeis and Samuel Warren's article "The Right to Privacy" dealt with a compilation of US decisions showing that privacy concerns are a serious offense to privacy violations. be human.

At the end of the 20th century, advances in computer technology and automated data processing began to take shape, so new legislation began to emerge and gain attention. "Around 1970, it was seen that legal decisions and legislation recognized that personal data were a projection of an individual's personality and, therefore, subject to legal protection (LUGATI; ALMEIDA, 2021).

In the 1980s, new data protection laws were implemented in France, Norway, Sweden and Austria. It was at this time that in 1981 the European Commission harmonized the rules for automatic data protection processing and the free flow of that data, resulting in the European Personal Data Directive, and in 2016 a new Regulation (EU) 2016/679, General Regulation of Data Protection.

Today in Brazil there is a legal diploma that deals with data protection, the LGPD, but before it came into force, even if by omission, data protection began to be treated by article 5º X of the Federal Constitution, guaranteeing privacy and security. . to the constitution, another This concept of protection was also initiated by scattered laws, such as the Consumer Protection Code when it comes to protecting the data of the holder of databases and habeas corpus data, see Danilo Doneda's guidance on the subject:

> The protection of personal data in the Brazilian legal system is not structured based on a unitary normative complex. The Brazilian Constitution addresses the problem of information initially through guarantees to freedom of expression and the right to information, which must eventually be confronted with the protection of personality and, in particular, with the right to privacy. Furthermore, the Constitution considers private life and intimacy inviolable (article 5, X), see specifically the interception of telephone, telegraphic or data communications (article 5, XII), as well as establishing the habeas data action (art. 5, LXXII), which basically establishes a type of right to access and rectify personal data. In infraconstitutional legislation, the Consumer Protection Code, Law 8,078/90, stands out, whose article 43 establishes a series of rights and guarantees for consumers in relation to their personal information present in "databases and records", implementing a systematic approach based on the Fair Information Principles to the matter of granting credit and enabling part of the doctrine to verify in this legal text the normative framework of the principles of personal data protection in Brazilian law. (DONEDA, 2021)

In short, data protection is new in Brazil, however, as explained, it is a subject that has been addressed for decades, mainly in Europe, in the search for the protection of private life and intimate rights. Changes in privacy, increased ability to collect, process and use information have changed the world, and concerns about uncontrolled amounts of information have created some laws and greater respect for privacy in society. The premise of Law No. 13,709/2018, which regulates the processing of personal data in Brazil, is to guarantee respect for private life in the community flow of personal data. As mentioned, its objective is to protect "fundamental rights

of freedom and privacy and the free development of the personality of natural persons". (BRASIL, 2018), includes digital media, does not exclude the physical environment, such as data in documents, resumes, forms and payroll. In article 2, the law defines its foundations, namely: privacy, self-determination of information; freedom of expression, information, communication and opinion; inviolability of intimacy, honor and image; economic and technological development and innovation; free Initiative; free competition. and consumer protection; human rights; the free development of the personality; the dignity of the natural person and the exercise of citizenship.

The holder of personal data is the natural person (individual) to whom the personal data is processed, it should be noted here that legal entities are not included, and article 5 of the LGPD also defines what personal data is, i.e. , "related to an identified or identifiable natural person" (BRASIL, 2018) and sensitive data, that is, "personal data relating to race or ethnicity, religious beliefs, political opinions, membership of trade unions or organizations of a religious, philosophical or political nature, data related to sexual life, genetic or biometric data, when related to natural persons" (BRASIL, 2018). Furthermore, the concept of therapy needs to be understood. LGPD claims:

> Article 5 - of information, modification, communication, transfer, diffusion or extraction" (BRASIL,2018).

Finally, the guiding principles of the Law are contained in its article 6, which, except by good will, describes the principle of purpose as "lawful, specific, clear and informed treatment of the data subject, no treatment incompatible with these purposes. possibility" (BRASIL, 2018), the principle of adequacy, "compatibility of the processing with the purpose for which the data subject was informed, depending on the context of the processing" (BRASIL, 2018), that is, that the data must be sufficient, relevant and relevant to your purpose It doesn't matter.

There are also the principles of necessity, described as "restricting processing to the minimum necessary to achieve its purposes, with the coverage of relevant data being proportionate to the purpose of data processing and not excessive"; the principle of free access, described as "restricting processing to the Guarantee, facilitated and free consultation on the form and duration of processing and the integrity of your personal data"; the principles of data quality, described as "guaranteeing data subjects of the accuracy, clarity, relevance and timeliness of their data, as necessary and fulfilling the purpose of its processing" (BRASIL, 2018), in which the principle explains that information incorrect information must be corrected, outdated or irrelevant information must be prohibited, or any data can be requested to be added to maintain the veracity of the information, based on this, it is possible to provide the best rights reserved by the holder.

There are also the principles of transparency, which give holders the right to the existence of data files; and management measures"; the precautionary principle, which translates as "measures to prevent damage resulting from the processing of personal data"; the principle of non-discrimination, which includes "processing is not possible for unlawful or abusive discriminatory purposes", data must be processed for certain purposes, these purposes must be communicated to the data subject. (BRAZIL, 2018)

Finally, the principle of responsibility is recognized in the law as "the agent's proof that effective measures have been taken that can demonstrate compliance with personal data protection rules, and even the effectiveness of these measures". (BRAZIL, 2018). Finally, a look at the importance of the new law for our national order:

> They are becoming the new inputs of the new economy, which can compromise not only the privacy of users, but also personal identity, informational self-determination, freedom, opportunities and perspectives of the present and future of people and democracy itself. (FRAZÃO, 2021)

And so, the General Data Protection Law entered our legal system, bringing many new features about personal data protection and drastically changing the way companies and public bodies treat the privacy and security of users' data who will have the right to adequate information.

5 LGPD AND OPEN BANKING: EVOLUTION OR VIOLATION?

Consent is a free and obvious declaration by the holder of personal data that their data is processed for a specific purpose. According to the LGPD, consent is "the free, informed and unequivocal expression of the holder's consent to the processing of their personal data for a specific purpose" (Brasil, 2020).

Freedom of expression refers to the holder's choice not to be imposed or bound; informed expression refers to the data subject's choice to consent to processing based on clear information, the concept of clear expression

involves a positive action on the part of the data subject, which leaves no doubt that they intend to consent to the processing of their personal data.

Therefore, it is the data subject's right, they must be given the freedom to choose what to do with their data, and this choice must be articulated for a specific and informed purpose. The LGPD requirements aim to guarantee data subjects the right to choose how their data will be processed and to comply with the fundamental principles established in the LGPD, especially with regard to informational self-determination, consumer protection, dignity and the exercise of privacy. citizenship as a natural person.

According to the LGPD, if the controller needs to share personal data after obtaining the data subject's consent, it must previously inform the data subject about the new processing method and obtain their consent for this new purpose. Furthermore, it is important to note that the burden of proof in relation to the collection of consent will lie with the person responsible for processing personal data, and that data processing in the context of consent bias is prohibited by the LGPD.

In addition to the right to express consent or not, data subjects also have other rights provided for in legal texts. Among them, a list of rights is mentioned in Chapter III of the LGPD, rights that derive from the principles of freedom, intimacy and privacy.

According to the text, the holder has the right to confirm and access their data and request correction if the data is incomplete, inaccurate or out of date, thus guaranteeing its quality; information about the possibility of not giving your consent and withdrawal of consent may be requested.

Furthermore, the LGPD allows holders to transfer their data to another service or product provider, a right that is occasionally confused with one of the objectives of Open Banking. In addition to protecting holders' control over their data, most of the holders' rights established in the LGPD make it possible to adjust and improve the offer of products and services to individuals, for example, the processing of complete data, and updating, optimizing the data market. credit and the basis of organic functioning, directly affecting financial markets and other sectors of the economy.

What are the situations in which individuals are required to transfer data to the bank? In addition to legislation throughout Brazil, the financial sector is subject to various sectoral regulations. Transfers of financial data from individuals to financial institutions can occur between financial institutions and consumers, as well as between financial institutions themselves.

The data exchange relationship between consumers and financial institutions is designed to serve the purpose of providing financial services, but can also support financial institutions in fulfilling their obligations to authorities and regulators. In some cases, financial institutions process and share consumer data due to the need to send information about illegal or abusive activities, in accordance with the terms of applicable laws and regulations, in accordance with Article 7(II) and Article 11(II) of the LGPD.

These shares can be offered to the sector's regulatory bodies, the Central Bank of Brazil (BCB), the Securities and Exchange Commission (CVM) and the Financial Activities Control Commission (COAF). According to Law No. 9,613/1998, there are actions that may provide evidence of crimes against the country's financial system, as examples of situations that lead to compulsory notification and, therefore, the sharing of personal data by financial institutions.

Furthermore, it is legal for financial institutions to exchange information relating to the consumer with other financial institutions to form databases, including those related to default, in which case the consumer protection law is in its art. Article 43 establishes the need for transparency and the consumer's right to access and rectification, and imposes requirements on its legality.

In this sense, the Active Registration Law (12,414/2011) regulates the formation and obligations in relation to credit history databases, amended by Complementary Law 166/2019. The changes expanded access to consumer data and established the possibility of automatically including consumer data (opt-in) and excluding it upon request (opt-out).

Here there is a contradiction with the LGPD on consent, but the LGPD provides a legal basis for credit protection to justify such data processing operations. Therefore, any conflict of laws may need to be resolved by the competent judicial authority. Furthermore, the ANPD guidelines help balance the legal basis for consent and credit protection. It should be noted that the exchange of information carried out by financial institutions must comply with bank secrecy requirements, as well as those established by the Central Bank of Brazil and the Commission of Securities, respecting the exceptions provided for in art. Article 1 of Law No. 105/2001.

The LGPD only conceptualizes personal data and sensitive data, and does not specify financial data throughout the text, which, Contrary to what many people think, they do not fall directly into the category of sensitive data. Financial data is often not sensitive data in itself, but depending on the context and how it relates to other personal data, this data can easily become sensitive data.

For example, data from personal credit transactions that indicate the purchase of medicines or payment for a consultation may be considered sensitive because they refer to the individual's health. The context in which financial data controllers analyze which data will be considered sensitive data is very important as stricter rules will apply to the processing of this data under the LGPD.

Before LGPD, financial data was already protected. The Bank Secrecy Law of 2011 (BRASIL, 2001) and BCB regulations, such as BCB Joint Resolution nº, relating to secrecy, confidentiality and data protection. Considering that there is no specific definition of the term "personal financial data" in the legislation, the concept will be constructed based on the Bank Secrecy Law, which provides in its § 1 that the secrecy of active and passive operations must be protected • Financial institutions and their services.

Therefore, taking into account the reasons presented, for the purposes of this report, we treat personal financial data as any information about an identified or identifiable natural person (as per LGPD guidance) in relation to active and passive financial transactions, and services provided.

These shares can be offered to the sector's regulatory bodies, the Central Bank of Brazil (BCB), the Securities and Exchange Commission (CVM) and the Financial Activities Control Commission (COAF). According to Law No. 9,613/1998, there are actions that may provide evidence of crimes against the country's financial system, as examples of situations that lead to compulsory notification and, therefore, the sharing of personal data by financial institutions. Furthermore, it is legal for financial institutions to exchange information relating to the consumer with other financial institutions to form databases, including those related to default, in which case the consumer protection law is in its art. Article 43 establishes the need for transparency and the consumer's right to access and rectification, and imposes requirements on its legality.

In this sense, the Active Registration Law (12,414/2011) regulates the formation and obligations in relation to credit history databases, amended by Complementary Law 166/2019. The changes expanded access to consumer data and established the possibility of automatically including consumer data (opt-in) and excluding it upon request (opt-out).

Here there is a contradiction with the LGPD on consent, but the LGPD provides a legal basis for credit protection to justify such data processing operations. Therefore, any conflict of laws may need to be resolved by the competent judicial authority. Furthermore, the ANPD guidelines help balance the legal basis for consent and credit protection. It should be noted that the exchange of information carried out by financial institutions must comply with bank secrecy requirements, as well as those established by the Central Bank of Brazil and the Securities and Exchange Commission, respecting the exceptions provided for in art. Article 1 of Law No. 105/2001.

The LGPD only conceptualizes personal data and sensitive data, and does not specify financial data throughout the text which, contrary to what many people think, does not fall directly into the category of sensitive data. Financial data is often not sensitive data in itself, but depending on the context and how it relates to other personal data, this data can easily become sensitive data.

For example, data from personal credit transactions that indicate the purchase of medicines or payment for a consultation may be considered sensitive because they refer to the individual's health. The context in which financial data controllers analyze which data will be considered sensitive data is very important as stricter rules will apply to the processing of this data under the LGPD.

Before LGPD, financial data was already protected. The Bank Secrecy Law of 2011 (BRASIL, 2001) and BCB regulations, such as BCB Joint Resolution nº, relating to secrecy, confidentiality and data protection. Considering that there is no specific definition of the term "personal financial data" in the legislation, the concept will be constructed based on the Bank Secrecy Law, which provides in its § 1 that the secrecy of active and passive operations must be protected • Financial institutions and their services.

Therefore, taking into account the reasons presented, for the purposes of this report, we treat personal financial data as any information about an identified or identifiable natural person (as per LGPD guidance) in relation to active and passive financial transactions, and services provided.

In this sense, both the BCB and the ANPD will play a fundamental role in supervising the management of the consent of institutions that are part of Open Banking and in transparency with holders, ensuring that institutions obtain the consent of holders and other complementary provisions in accordance with the LGPD.

Therefore, it is necessary for laws and regulations to communicate with each other, to avoid regulatory errors, especially for malicious agencies to find loopholes in laws or regulations to process personal data that are inconsistent with the reasons presented by the LGPD. data quality, transparency and non-compliance Applicability of the principle of discrimination.

In its article 6, the LGPD links its main objectives and lines of action to common principles existing in different legal systems (Brazil, 2010). In this article, the law establishes 10 foundations to guide its provisions of the LGPD, stating that the processing of personal data must be guided by good faith and the following principles: purpose, sufficiency, necessity, free access, data quality, transparency, security, prevention, Non-Discrimination and Responsibility and Accountability (Brazil, 2020).

For example, the LGPD contains provisions that support the need to process data for a lawful, specific, clear and informed purpose (principle of necessity), and that such processing must be carried out in a compatible way (principle of adequacy) to inform data subjects purpose (principle of transparency).

Furthermore, in each processing operation, data must be kept accurate, clear, relevant and up-to-date

(Principle of Data Quality), respecting the fact that the processing of data is not intended for unlawful or abusive discriminatory purposes (Principle of Non-Discrimination, Discrimination Compliance). Specifically, taking into consideration the topics covered in this report, as well as BCB Joint Resolution 4,658/2018, we will follow the principles of data quality, transparency and non-discrimination also mentioned in article 4 of the Resolution, articles I, III and item IV.

The principle of transparency is closely related to a financial institution's relationship with its customers, as it guarantees holders not only clear and accurate information, but also specific and truthful information. Furthermore, even though commercial and industrial secrets are protected, they must not override the rights of holders and other fundamental principles and principles of the LGPD.

Holder transparency will be one of the main points of observation for the smooth functioning of Open Banking, and will be a challenge in the first place, as it is directly related to the effective management of holder consent and the need to optimize mapping data activities to ensure that clear holders know exactly how their personal data is processed.

Data quality is also another aspect that must be observed with great caution in the context of open banking, especially on topics related to data relevance and minimization. This will require data controllers to create rigorous ongoing verification procedures for accuracy, clarity, relevance and currency of data subjects.

The objective is to be faithful to the therapeutic purpose that informs the data subject and to avoid algorithms that use inaccurate, outdated and irrelevant data to make automated decisions. The focus on data quality is faithfully linked to the principle of non-discrimination, as low data quality affects not only equality between individuals, but other fundamental rights protected not only by the LGPD, but also by the Federal Constitution.

However, the most visible and most studied effect related to rights affected by poor data quality is non-discrimination. Several studies and reports involve the use of unrepresentative data or biased algorithms that treat people unequally based on skin color, race, gender, sexual orientation, religion, and more. Therefore, if structured measures that value data quality are not created and the necessity and appropriateness of processing are not validated, the result of automated decision-making can differentiate people based on their sensitive data. From an open banking perspective, data relating to skin color, gender and origin can further influence decisions on granting credit by financial institutions (França, 2019). News was published about the discovery of machismo and racist replication by algorithms, mainly in the banking market. 55 As all data from financial institutions is consolidated, the right to non-discrimination may be more affected, maximizing systemic bias.

With this in mind, regulators should not only focus on personal data itself, but should also develop methods to educate both the public and private about how algorithms related to open banking systems will work, so that the basis of the algorithms - data - may be limited by legislation and the logic, principles and limitations of regulations. Once again, oversight by public authorities will be crucial.

CONCLUSION

As Open Banking presupposes consent, which is one of the legal foundations of the LGPD, customers can grant permission to share at any time or revoke it. It is worth noting that this acceptance is specific, that is, customers only allow certain data to be shared with third-party banks, and it is not universally applicable to all data or all institutions.

To share this information with other agencies, you will need to collect a new subject consent form. This means that the body receiving the data will assume the role of controller under the LGPD.

Therefore, specific bodies must transparently control the storage process of this data, in addition to providing effective and practical services to data subjects who withdraw their consent or request any clarification regarding the processing of their information. This new process can be facilitated by using a customer relationship management (CRM) system and other management tools.

Creating records to show how and where this personal data is collected is a legal obligation that reflects the importance of transparency for financial institutions. Companies must also have an information retention policy that meets legal requirements. In this case, consent will be the legal basis for retaining certain data until its revocation or expiration.

Therefore, the processing of personal data will become a fundamental standard that financial institutions need to consider when joining Open Banking. As the banking market innovates and must follow the development of solutions that respect privacy and protect personal data, new processes and demands will emerge.

REFERENCES

BARBERIS, JN; BUCKLEY, R.P.; ARNER, DW FinTech, RegTech, and the Reconceptualization of Financial Regulation. Northwestern**Journal of International Law & Business,**v. 37, no. 3, 2017.

BARBERIS, JN; BUCKLEY, R.P.; ARNER, DW The Evolution of Fintech: A New Post-Crisis Paradigm? University of Hong Kong**Faculty of Law Research Paper**No. 2015/047, 20 Oct. 2015.

BRAZIL, Central Bank of Brazil,**Resolution No. 4,658**April 26, 2018.

BRAZIL, Central Bank of Brazil,**Resolution No. 4,658**of April 26, 2018. Provides for the implementation of the Open Financial System (Open Banking).

BRAZIL, Central Bank of Brazil.**Joint Resolution No. 1**May 4, 2020.

BRAZIL, Complementary Law nº105, of January 10, 2001.**Bank Secrecy Law.**Provides for the confidentiality of the operations of financial institutions and provides other measures

BRAZIL.**National School of Consumer Protection**The protection of personal data in consumer relationships: beyond credit information / National School of Consumer Protection; prepared by Danilo Doneda. – Brasília: SDE/ DPDC, p. 43, 2010.

BRAZIL. Federal government.**Guide to Good Practices for Implementation in Federal Public Administration.**1 v.11, 2020.

BRAZIL. Federal government.**Guide to Good Practices for Implementation in Federal Public Administration.**1 v.21,2020

CUEVA, Ricardo Vilas Boas. Insufficient protection of personal data in Brazil. Contemporary Civil Law Magazine-RDCC: **Journal of Contemporary Private Law**, n. 13, p. 61, 2017.

DENZIN, N.; LINCOLN, Y.**Handbook of Qualitative Research.**London: Sage Publication Inc, 2000.

EUROPE. EDPS.**Guidelines on data protection in EU financial services regulation**. P. 5

FRANCE. European Union Agency for Fundamental Rights. Data quality and artificial intelligence–mitigating bias and error to protect fundamental rights. P. 8, 2019

GOETTENAUER, C. Open Banking and the Platform Banking Model: the need to reassess the legal definition of banking activity. Magazine of the Attorney General's Office of the Central Bank, [Sl], v. 14, no. 1, p. 13-27, Sept. 2020

KÖCHE, J.C.**Fundamentals of Scientific Methodology:**theory of science and initiation to research. 29. ed. Petrópolis: Voices, 2011.

MAGNUSON, WJ Regulating Fintech.**Vaderbilt Law Review,**2017

MARCONI, MA; LAKATOS, IN Fundamentals of scientific methodology. 7.ed. São Paulo: Atlas, 2010.

MARTINS, Leonardo (Org.). Fifty years of jurisprudence of the German Federal Constitutional Court. Montevideo: **Konrad Adenauer Foundation**, 2005, pp. 233-235

REYNOLDS, Faith.**Open Banking:**a consumer perspective. UK Open Banking, p. 18-19, 2017.

SHANK, G. Qualitative Research.**The Personal Skills Approach**. New Jersey: Merril Prentice Hall. 2002.

VIOLA, M.; HERINGER, L. Portability in the General Data Protection Law.**Institute of Technology and Society,** 2020.