https://doi.org/10.53303/hmc.v15i1.1251
ISSN 2526-6349 *On-line version*
ISSN 2175-1943 *Print version*

Original article

Conformidade dos contratos de adesão das plataformas virtuais com a Lei Geral de Proteção de Dados

Compliance of virtual platform membership contracts with the General Data Protection Law

Nayne Yasmin Souza Neves[1] | **Marcus Vinicius Ramos de Jesus**[1] | **Antonio Luiz Nunes Salgado**[1]

[1]Centro Universitário FUNORTE, Montes Claros, MG, Brazil.

Abstract

Objective: to analyze the compliance of adhesion contracts on virtual platforms with the General Data Protection Law (LGPD). **Materials and Methods:** the research adopted a qualitative approach, based on the documentary analysis of privacy policies from Meta, Google, X, and TikTok. The criteria used for analysis were: consent, transparency, data sharing with third parties, and data security and storage. **Results:** it was found that, although all platforms claim compliance with the LGPD, there are still gaps regarding the clarity of consent collection, language accessibility for the public, detail about third parties, and effective security mechanisms. The generalization and imposition of full acceptance compromise the validity of consent. **Conclusion:** the analyzed platforms do not fully comply with the provisions of the LGPD. The superficial nature of privacy policies may lead to flawed consent, rendering contracts voidable and giving rise to civil liability. As adhesion contracts, they may also infringe consumer rights. The study highlights the need for reformulating these policies to ensure clarity, granularity, and accessibility, and underscores the supervisory role of the National Data Protection Authority (ANPD) in enforcing corporate compliance.
Keywords: Adhesion contracts. Consumer Protection Code. General Data Protection Law. Privacy.

Resumo

Objetivo: analisar a conformidade dos contratos de adesão em plataformas virtuais com a Lei Geral de Proteção de Dados (LGPD). **Materiais e Métodos:** abordagem qualitativa, fundamentada na análise documental de políticas de privacidade das plataformas Meta, Google, X e TikTok. Foram utilizados como critérios de análise: consentimento, transparência, compartilhamento com terceiros, segurança e armazenamento de dados. **Resultados:** embora todas as plataformas declarem adequação à LGPD, ainda existem lacunas quanto à clareza na coleta de consentimento, linguagem acessível ao público, detalhamento sobre terceiros e mecanismos efetivos de segurança. A generalização e a imposição do aceite integral comprometem a validade do consentimento. **Considerações finais:** as plataformas analisadas não demonstram plena conformidade com os dispositivos da LGPD. A superficialidade das políticas de privacidade pode configurar vícios de consentimento, passíveis de anulação contratual e responsabilização civil e, tratando-se de um contrato de adesão, pode ferir os direitos dos consumidores. Compreendeu-se a necessidade de reformulação das políticas, tornando-as claras, granulares e acessíveis e do papel fiscalizador da ANPD para garantir o efetivo cumprimento pelas empresas.
Palavras-chave: Contratos de Adesão. Código de Defesa do Consumidor. Lei Geral de Proteção de Dados. Privacidade.

Corresponding author: Antonio Luiz Nunes Salgado| antonio.salgado@funorte.edu.br
Received on: 07|31|2025. Approved on: 01|10|2026.
Evaluated by a double- blind review process.

How to cite this article: Neves NYS, Jesus MVR, Salgado ALN. Compliance of virtual platform membership agreements with the General Data Protection Law. Humanidades (Montes Claros). 2026;15:e1251. https://doi.org/10.53303/hmc.v15i1.1251

Introduction

With the advent of the digital age and the consequent emergence of consumer relations in this sphere, virtual platforms are playing an important role in commercial relations and increasingly entering people's daily lives. In this scenario of massification, adhesion contracts have become a legal instrument that aims to facilitate the formation of mass businesses, characterized by uniformity, predetermination, and rigidity, forcing the adherent to "acceptance in blocks", as defined by Gomes[1]. This has become a reality in virtual business.

In 2018, the General Data Protection Law (LGPD, acronym in Portuguese) was enacted. With this law, there arose a need to analyze commercial practices conducted on virtual platforms that use adhesion contracts to protect consumers' personal data. It is necessary to assess whether such adhesion contracts imposed on consumers through a simple "read and accept" comply with the LGPD, considering the standard's transparency requirements.

For this article, we sought to analyze whether the membership agreements of virtual platforms comply with the rights protected by the LGPD. The contracts drawn up and used by the main virtual platforms in Brazil—Google, Meta, X (formerly Twitter), and TikTok—were investigated to assess whether consumer data is, in fact, protected and to what extent they comply with the LGPD. Secondarily, the objective was to evaluate whether the contracts guarantee privacy and data protection in digital consumer relations.

In assessing potential non-compliance, it also highlights the importance of data protection in all virtual contracts. This is because the widely held view is that users are not concerned about sharing their personal data or the possible consequences of its use.

Material and Methods

The methodology chosen to guide the study was based on a qualitative approach, focusing on the analysis of samples of membership agreements that were made available on the virtual platforms themselves. The procedure began with the collection of samples of membership agreements, using the criterion of the most widely used platforms in Brazil, namely Meta, Google, X, and TikTok.

The approach defined was qualitative, defined by Oliveira, Barros, and Souza[2] as one that "seeks to interpret the meanings, phenomena, and significance that people attribute to them, based on a variety of empirical studies." Thus, we sought to analyze the phenomena from the perspectives of the subjects involved.

For the analysis, the main criteria established in the LGPD were used: a) Consent of the data subject; b) Transparency in data collection; c) Sharing with third parties; d) Data security and storage. For each of these parameters, the research determines whether the contracts comply with the LGPD,

identifying patterns and differences among the selected contracts relative to the standard. The procedure sought to ensure greater credibility of the results.

Results

Initial aspects

Contracts are agreements between two or more parties seeking to create, modify, or terminate a legal relationship, according to Coelho[3], who also defines them as "a bilateral or multilateral legal transaction that creates obligations for one or all parties, to which correspond rights held by them or by third parties." This definition highlights the importance of the principle of the autonomy of will in the formation of contracts, which binds the parties to the contract, and characterizes equality so that both sides can negotiate, create, and modify the clauses as they see fit, provided they are civilly capable of forming legal transactions.

Article 104 of the Civil Code (CC)[4] determines that, for a legal transaction to be valid, it is essential to have (I) a capable agent; (II) a lawful, possible, and determined or determinable object; and (III) a form prescribed or not prohibited by law. In addition to the agent's capacity, a contract must be lawful for it to be considered valid. The lawfulness of the object and obligations determines that the contract cannot have an object that is contrary to the law; it must be possible, in the physical and legal sense of the word, and something that does not exist cannot be the object of a contract. And the object must be determined or determinable, that is, the object must be determined or, at least, details must be provided that enable its future determination[3].

Adhesion contracts, on the other hand, are defined by their unique structure and are governed in Brazilian law by the Consumer Protection Code (CDC, acronym in Portuguese), which distinguishes them from other contracts in that they do not require mutual agreement between the parties. They are notable for clauses established unilaterally by the proposer, with the adhering party having only the option to accept or reject their content. There is no real chance of making any changes to what is being agreed upon. "Art. 54 An adhesion contract is one whose clauses have been approved by the competent authority or established unilaterally by the supplier of products or services without the consumer being able to discuss or substantially modify its content"[5].

The express mention of the CDC in the adhesion contract, but not in the CC, as in other modalities, stems from the fact that the Brazilian legal system aims to ensure protection for the weaker party in the relationship, the adhering consumer. These contracts are designed to serve many people and are therefore standardized, since the contract is drawn up unilaterally and rigidly, due to the impossibility of altering its content, as stated by Gomes[1].

It should be noted that, precisely because the adherent receives the predetermined contract without the possibility of changing the clauses, there is an imbalance in the consumer relationship. The adherent's vulnerability vis-à-vis the proponent becomes clear. According to Coelho[3], if the consumer wants to enter the contract, they have no alternative but to agree to the supplier's terms and conditions, with no room for negotiation.

With the migration of legal business to the internet, especially with the growing use of virtual platforms, social networks, and e-commerce, there has been a transformation in contractual relationships. Virtual commerce has driven the use of electronic contracts. For the purchase of products or services, internet-based transactions require, as a central step, the execution of virtual contracts, almost all of which are adhesion contracts. This includes electronic services for the use of and access to virtual platforms. Their privacy policies function as adhesion contracts, imposing unilateral conditions on users who adhere.

Therefore, just like conventional contracts, electronic contracts are also based on the free will of two or more people to create, modify, or terminate a legal relationship, but in the digital sphere. Barbagalo defines them as "electronic contracts being agreements between two or more persons to establish, modify, or terminate a legal relationship of a patrimonial nature, expressing their respective declarations of will through interconnected computers."[6]

The regulatory gap regarding personal data and privacy policy in Brazil, filled in 2018 with the LGPD[7], came into force in 2020, regulating the collection and storage of data in browsers, operating systems, and devices.

> Art.1st. This Law provides for the processing of personal data, including in digital media, by natural persons or legal entities governed by public or private law, with the aim of protecting the fundamental rights of freedom and privacy and the free development of the personality of natural person[7].

The LGPD emerged as a highly impactful standard, concentrating regulatory standardization in Brazil on personal data protection. The legislation brought about an important shift in how companies in general handle (collect, store, and use) personal data. Thus, in the growing context of the use of electronic contracts, often without individuals being aware that they are entering into a contract, through a simple "I have read and accept," this regulatory standard plays a central role in regulating these rights. The use of digital platforms, some of which are entertainment-oriented, can mask the formal aspect of contracting, since it does not initially appear to be an onerous exchange.

To analyze its applicability and verify whether the main virtual platforms operating in the national territory comply with legal provisions aimed at protecting personal data, it is essential to understand the main rights regulated by the LGPD[7], listed below:

Consent: defined in Article 5, item XII, of the LGPD as “a free, informed, and unequivocal statement by which the data subject agrees to the processing of their personal data for a specific purpose.” Article 7 reinforces that processing can only occur with the consent of the data subject, except in specific cases provided for by law[7].

Transparency: provided for Article 6, item VI, and regulated by Article 9, guarantees the data subject easy access to information about the processing of their data, such as the purpose, form, duration, identification of the controller, shared use, and rights of the data subject[7].

Data sharing: According to Article 5, item XVI, of the LGPD, this is the communication, dissemination, or transfer of personal data between public and private entities. Article 7, §5 of the aforementioned law provides for the need for the data subject's consent for sharing with third parties[7].

Security and storage: Regarding security, as provided for in Article 6, item VII, and Articles 46 and 47 of the LGPD, operators must implement technical and administrative measures to protect personal data from unauthorized access and incidents such as loss, destruction, and improper disclosure. As for storage, the LGPD provides in its article that data should only be stored until its purpose is achieved[7].

The above definitions will form the basis for the analysis of the adhesion contracts of the selected platforms, also known as “privacy policy,” which will be presented in the following topic.

Data collection from selected platforms

For this article, we analyzed the privacy policies of the virtual platforms Meta, Google, X (formerly Twitter), and TikTok to verify their compliance with the LGPD established criteria. The choice of these companies' privacy policies is based on the popularity of their virtual platforms. In the case of Meta, for example, it owns three of the most widely used platforms in the country (WhatsApp, Instagram, and Facebook), with a privacy policy that covers all of them. According to the website's report, these are the social networks and digital services with the highest number of visits and time spent in Brazil.

The analysis focused on the following criteria: consent, transparency in data collection, sharing with third parties, and security and storage. The table below presents excerpts from the privacy policies, a small sample of how these criteria were standardized by the virtual platforms subject to the study.

Chart 1. "Excerpts from platform regulatory documents by evaluation criterion."

Consent	META	"When you use our Products, we collect some information about you, even if you don't have an account." "You can also manage your information by accessing the settings of the Products you use. You may also have other privacy rights under applicable laws."
	GOOGLE	"The information collected by Google and how that information is used depends on how you use our services and how you manage your privacy controls."
	X	"To use some of our products and services, you need to have an account, and to create an account, you need to provide us with certain information."
	TIKTOK	"You have rights and choices when it comes to your information. You may be entitled to certain rights under applicable laws, which may include the right to access, delete, update, or correct your data."
Transparency	META	"We use the information we collect to provide you with a personalized experience, including advertisements, along with the other purposes explained in detail below.
	GOOGLE	"We use the information we collect across all our services for the purposes described below: to provide our services, maintain and improve our services, develop our services [...]."
	X	"When you use our services, we collect information about how you use our products and services. We use this information to provide you with products and services, to help keep X safer and more respectful for everyone, and to make it more relevant to you.
	TIKTOK	"We may update this Privacy Policy from time to time. When we update the Privacy Policy, we will notify you by updating the "Last Updated" date at the top of this policy and posting the new Privacy Policy or providing any other notice required by applicable law. Your continued access or use of the Platform after the date of the updated policy constitutes your acknowledgment of the updated policy. If you do not agree with the updated policy, you should stop accessing or using the Platform."
Sharing with third parties	META	"We do not sell your information to anyone, and we never will. We also require partners and other third parties to follow rules about how they use and disclose the information provided. Here are more details about the people with whom we share information: partners and suppliers."
	GOOGLE	"We share personal information outside of Google when we have your consent. For example, if you use Google Home to make a reservation with a reservation service, we will ask for your permission before sharing your name or phone number with the restaurant."
	X	"We may share your information with our service providers who perform functions and provide services on our behalf, including payment service providers that facilitate payments; service providers that host our various blogs and wikis [...]" "We share or disclose your information with your consent or at your direction, for example, when you authorize a third-party web client or application to access your account or when you direct us to share your feedback with a company."
	TIKTOK	"We share your information with the following parties: Business partners, Service providers, Advertisers, advertising networks, and measurement partners, Independent researchers, Our corporate group, For legal reasons."
Data security and storage	META	"We retain information for as long as necessary to provide our Products, comply with legal obligations, or protect our interests or those of others. We decide how long we need it on a case-by-case basis."
	GOOGLE	"All Google products are developed with robust security features that continuously protect your information." "We retain the data we collect for different periods of time, depending on what the data is, how we use it, and how you have configured your settings."
	X	"We retain different types of information for different periods of time, depending on how long we need to retain it to provide our products and services, to comply with our legal obligations, and for security reasons." "To protect your privacy and maintain security, we take steps to verify your identity before granting you access to your personal information or responding to a deletion, portability, or other related request."
	TIKTOK	"Your information may be stored on servers located outside the country where you live, such as Singapore, Malaysia, Ireland, and the United States. We maintain key servers around the world to provide our services globally and continuously." "We take steps to ensure that your information is treated securely and in accordance with this policy. Although we use reasonable measures to protect your personal data, for example, through encryption, we cannot guarantee the security of your information transmitted through the Platform; any transmission is at your own risk."

Elaborated by the authors using the regulatory documents available on the websites of each digital platform[8-11].

After this brief presentation of how criteria are set out in privacy policies, it was possible to note that, regarding consent, all privacy policies require users to accept the terms of use and the privacy policy. Meta and Google provide more details, informing users that they can manage such information in specific tabs on the platforms, while TikTok and X use more generic terms, stating only that, with use, it will be necessary to provide information. Consent has become implicit in the continued use of the platform, which does not fully comply with the LGPD's requirement for clear, explicit, and unambiguous consent; using continued use as consent is not clear or specific.

In terms of transparency, Google is the platform that provides the most detailed information about data processing, the purpose of processing, and the means of collection. Meta, on the other hand, uses generic expressions such as “information about how you use our products” or “interactions with partners,” without clearly explaining what specific data is collected in these interactions. TikTok also uses vague terms such as “other information you provide to us,” and gives users the option to agree to the terms or stop using the platform. As for X, the information is provided in technical terms, such as IP address, browser, and operating system, without explaining how this processing is carried out.

Regarding data sharing with third parties, all companies state that such sharing occurs and requires consent. Google and X inform the categories of sharing, but Google provides more detail about who these third parties are and the reason for sharing. X categorizes with general information, and Meta mentions sharing between companies in the same economic group, advertising partners, service providers, and researchers, but often uses generic expressions such as “authorized third parties” without detailing specific sectors or names. TikTok states that it shares this data and its purpose, but, also does so without providing further details or options to the user.

When it comes to data security and storage, Google once again has the most detailed privacy policy, clearly stating that it has data centers in various locations around the world and clarifying the retention period for this data, which varies by data type and purpose. Meta and TikTok also state that data may be stored on international servers and clarify that data may be stored for as long as necessary to achieve its purpose or for the time defined by law. X does not specify storage locations, only stating that security is provided through encryption and access control.

This overview highlights the differences between platforms, providing a clearer understanding of which are more compliant with LGPD principles, and which require substantial improvements to their privacy policies. Furthermore, it should be noted that, even when complying with legal requirements, some privacy policies are written in a generic manner, failing to specify essential points for user understanding.

Discussion

By analyzing the privacy policies on Google, Meta, X, and TikTok, it was possible to identify gaps between the content of these policies and the provisions of current legislation. Although there is a clear effort by the platforms to align their privacy terms with the LGPD, there are still considerable loopholes, more pronounced in some policies than in others, highlighting the need for substantial improvements.

Even with the formalization of the commitment to Brazilian legislation for operating in the national territory and the attempt to demonstrate compliance in a post-LGPD context, especially considering the intensification of virtual relationships, there remains a gap between what is provided for in the policies and the practical reality of personal data processing. These gaps can be remedied by more detailed, accessible privacy policies that clearly and precisely outline the essential aspects of data processing.

In general, there is a tendency toward omission or superficiality in the points privacy policies address, making them generic and uninformative. Although some of the platforms investigated, such as Google, provide greater detail, there is still room for improvement[7]. This point should be given special consideration because the target audience for these policies is largely composed of lay users who lack the technical or legal knowledge to fully understand the terms used. Thus, privacy policies must be written in clear, objective language with adequate explanations.

We sought to deepen discussion on the criteria analyzed, which are central to the LGPD.

Initially, regarding consent, defined by Hale[12] as "a free, informed, and unequivocal statement by which the data subject agrees to the processing of their personal data for a specific purpose." In accordance with the legislation itself, which requires consent to be expressed, that is, clearly consciously manifested by the holder.

Although the platforms analyzed state in their privacy policies that user consent is required for data processing, in practice, this requirement is often fulfilled in a generic, conditional manner. This condition is evident, for example, in the case of TikTok, which requires full acceptance of the privacy policy as a prerequisite for accessing and using the service: "Your continued access or use of the Platform after the date of the updated policy constitutes your acknowledgment of the updated policy. If you do not agree with the updated policy, you must stop accessing or using the Platform."[10]

These policy models do not allow users to select which types of processing they consent to or not, that is, they do not fully comply with the legislation, as they create for the user the need to either fully accept or not use the services, since they do not allow for the possibility of consenting to the processing of some data and not others, with a strong tendency toward generalization of consent, without the necessary granularity established in the legislation.

Furthermore, even if the law requires express consent, the way in which this consent is collected may lead the data subject to a misperception of the actual extent of their agreement. This undermines the legitimacy of consent given in this manner, since the simple act of clicking on a button that says, “I have read and accept”, without any emphasis on the consequences of the processing or the possibility of simplified consultation, reduces consent to a mechanical act, without reflection on the part of the user. This trivialization of consent can render it ineffective, contributing to many data subjects consenting without full knowledge of the consequences, the purpose of the processing, and the destination of their data, adhering to a service that will process their data without their knowledge of the purpose and manner.

It should also be noted that, despite being provided for in current legislation, revoking consent is difficult, and there are obstacles to the platforms surveyed. This information is rarely addressed in privacy policies. As a result, if the user attempts to revoke consent for certain types of processing, there are conditions that prevent them from continuing to use the services, as the processing of many services is carried out in blocks, making it impossible for the user to specify what they consent to and what they do not. Another point is that acceptance is directly linked to the ability to use the services, leaving the data subject with the choice of consenting to the processing of all data or not using the services.

It should be noted that consent obtained from minors would be considered a null civil act pursuant to Article 166, I of the Civil Code, as it is a contract, and the LGPD provides in Article 14 that specific consent is required from at least one of the minor's parents. Obtaining this consent directly, without verifying age or obtaining authorization from the legal representative, constitutes not only a violation of the LGPD but also the nullity of the act[4,7].

It was then understood that the main problems regarding consent lie in how it is obtained and the lack of granularity in acceptance. Since it is up to the user to accept them in full or not to use the websites, in the first case, this problem of obtaining consent should be expressed, but in general, it boils down to a mechanical act. This condition weakens the act itself, rendering the contract voidable, under Article 171, II of the CC, since the way consent is obtained leaves ample room for defects of consent[4].

Regarding transparency, it follows Hale's definition as “a guarantee to data subjects of clear, accurate, and easily accessible information about the processing and the respective processing agents.”[12] The main obstacle identified in the privacy policies analyzed was the difficulty of accessing the language, which violates the definition of transparency addressed by doctrine and by the legislation itself.

Many of the documents use legal or technical terms that make them difficult for the public to understand, which is mostly composed of lay people without technical knowledge. In addition, there is a recurring use of vague and generic expressions, such as “we may share your data with trusted partners” or “we process your data to improve our services”, which compromise clarity and results in partial information. This lack of transparency is insufficient, preventing the data subject from fully understanding how their data is collected, used, stored, and eventually shared, contrary to the provisions of Article 6, item VI, of the LGPD[7].

Therefore, even though all platforms claim to comply with Brazilian data protection legislation, their privacy policies, in practice, do not ensure effective, clear, and sufficient communication with data subjects, which directly contradicts the principle of transparency. This concerns a scenario in which consent and informational self-determination depend directly on the user's ability to understand the potential consequences of using their personal data. The lack of full transparency not only violates data protection legislation but also weakens the legal reliability of the business that platforms can conduct, as everyone in the business chain may be held liable.

When it comes to sharing with third parties, significant gaps were identified in the privacy policies of the platforms analyzed, especially regarding transparency and the specification of information. Although all of them mention that personal data may be shared with “partners,” “affiliates,” or “service providers,” they present this information in a superficial and generic way, without identifying exactly who these third parties are, what data will be shared, and for what specific purposes. This omission violates the principle of transparency, as detailed above, and weakens the data subject's control over their data, compromising informed consent.

Furthermore, when analyzing the policies adopted by companies regarding security, defined by Hale[12] as “the use of technical and administrative measures to protect personal data from unauthorized access and from accidental or unlawful situations of destruction, loss, alteration, communication, or dissemination.” It is possible to note that, although the legislation expressly establishes that such companies must guarantee the security of the data provided by users and that their policies establish certain rules regarding security, these regulations are generic in terms of the mechanisms adopted, and there are also privacy policies that provide for exemption from security liability in certain cases, such as TikTok, which directly contravenes the provisions of the legislation.

It was possible to identify a structural problem in the analyzed privacy policies, since the omission of one of the criteria established by the LGPD compromises the others in a chain reaction. This is because these criteria do not operate in isolation, but in a dependent manner. Thus, the lack of clarity in the language affects the validity of consent, the inaccuracy in data sharing compromises

transparency, and the generalization of terms weakens the data subject's informational self-determination.

Noting that these privacy policies constitute a unilateral legal instrument with pre-established clauses, it is essential to recognize them as adhesion contracts, as regulated by Article 54 of the CDC, noting the possible flaws in obtaining consent, as any contractual instrument may present defects that lead to its annulment or full nullity, as provided for in Articles 171 and 161 of the CC, given that such policies have been showing a generic trend[4,5].

The LGPD requires that the processing of personal data be based on valid legal grounds set forth in Article 7, with free, informed, and unambiguous consent, especially in the case of sensitive data and data on children and adolescents, in accordance with Article 14. Failure to comply with these obligations, when proven, may result not only in the annulment of the contract, but also in civil liability for damages caused, pursuant to Article 927 of CC[4,7].

It should also be noted that failure to comply with the legal obligations imposed by the LGPD results in administrative sanctions provided for in Article 52, such as warnings, fines, suspension, or prohibition from performing activities related to data processing. In addition, Article 42 of the LGPD guarantees data subjects the right to full compensation for property, moral, individual, or collective damages, reinforcing the possibility of civil reparations provided for in the CC[7].

In line with this, the National Data Protection Agency (ANPD), created alongside the LGPD, has been overseeing data protection in Brazil since the legislation took effect. It has regulatory, supervisory, and sanctioning powers, and is responsible for issuing guidelines and initiating investigation procedures in cases of violations of the LGPD[13].

Since its creation, the ANPD has intensified its regulatory role regarding large digital platforms, as evidenced by reports and inspection procedures targeting Meta, TikTok, and X (formerly Twitter). The Authority's analyses pointed to a lack of compliance with data processing practices, particularly about transparency, the legal basis for processing, and obtaining valid consent[14].

These inspections reinforce that simply providing privacy policies does not guarantee compliance with the LGPD. In addition to these reports by the ANPD (acronym in Portuguese), there are other similar rulings. For example, the TJMA (Court of Justice of Maranhão) ordered Google, together with Apple, to pay R$ 19 million for violating the LGPD by making available an application that collected data irregularly and without the proper consent of users[15]. Although Google has not yet been directly fined by the ANPD, the court ruling demonstrates non-compliance with the LGPD.

Final Considerations

Based on a qualitative analysis of the privacy policies of Meta, Google, X, and TikTok, it was found that, although these companies are making efforts to comply with LGPD requirements, there are still significant gaps to be addressed. The main deficiencies are found in consent, especially in the way it is obtained. As for transparency, the language used in the policies is often inaccessible to most of the population, and there is still a problem with the generalization of the purposes of data processing and sharing with third parties without proper specification.

From the perspective of adhesion contracts, it is essential that these policies comply with the LGPD, under penalty of nullity, considering the potential defects of consent. Furthermore, when it comes to minors, obtaining consent without proper legal representation may result in absolute nullity, due to a direct violation of Article 14 of the LGPD[7] and the possibility of nullity provided for in Article 166, item I, of the CC[4].

The ANPD's actions have been essential in curbing abusive practices. This is evident in reports prepared on the Meta, X, and TikTok platforms, which highlight flaws such as insufficient granularity and lack of transparency, aspects already highlighted in this study. However, these reports have not yet been sufficient to drive the adoption of safeguards and the complete compliance of these platforms with current legislation, which is why the application of the sanctions provided for in the LGPD may be the next step, imposing measures ranging from administrative measures to civil liability for any moral and material damages resulting from legal non-compliance, as already adopted and widely applied by the Brazilian legal system.

It should be noted that the issue raised by this research must necessarily be combined with the platforms' own interests, since the reliability of their users in managing their personal data must be one of the pillars of their use. And also, because the penalties under Article 52 of the LGPD can reach up to fifty million reais and even the suspension of their operations[7].

Thus, it can be observed that the Brazilian legal system is moving towards the consolidation of a culture of data protection. Although gaps remain, the LGPD represents a significant step forward by establishing accountability and enforcement mechanisms, as well as encouraging the reformulation of privacy policies by digital platforms. Thus, it can be concluded that such companies have not fully complied with the legislation, having very generic policies, but through its control and sanctioning instruments, the legislation is managing to consolidate itself.

Authors´ contributions

Research conception and design: Nayne Yasmin Souza Neves; Marcus Vinicius Ramos de Jesus. Data collection: Nayne Yasmin Souza Neves; Marcus Vinicius Ramos de Jesus. Data analysis, interpretation, and manuscript writing: Nayne Yasmin Souza Neves; Marcus Vinicius Ramos de Jesus. Critical review of the

manuscript for intellectual content and final presentation: Nayne Yasmin Souza Neves; Marcus Vinicius Ramos de Jesus; Antonio Luiz Nunes Salgado. The authors approved the final version of the manuscript and declared themselves responsible for all aspects of the work, including ensuring its accuracy and integrity.

Conflict of interest

The authors declare no conflicts of interest.

References

1. GOMES. Orlando, **Contratos**. Rio de Janeiro: Forense, 2009.

2. OLIVEIRA, Ellen Synthia Fernandes de; BARROS, Nelson Filice de; SOUZA, Dayse Cristine Dantas Brito Neri de (org.). **Metodologias qualitativas em diferentes cenários: saúde e educação** [recurso eletrônico]. Goiânia: Gráfica UFG, 2018. 325 p.14.

3. COELHO, Fabio Ulhoa, **Curso de Direito Civil: Contratos**. v. 3. São Paulo: Thomsom Reuters Brasil Conteúdo e Tecnologia LTDA, 2020.

4. BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. **Institui o Código Civil**, Brasília, DF: Presidência da República, Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 18 maio 2025.

5. BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Dispõe sobre a proteção do consumidor e dá outras providências**. Brasília, DF: Presidência da República, 1990. Disponível em: https://legislacao.presidencia.gov.br/atos/?tipo=LEI&numero=8078&ano=1990&ato=376UTRq1keFpWTab7. Acesso em: 18 maio 2025.

6. BARBAGALO, Erica Brandini. **Contratos eletrônicos: Contratos formados por meio de redes de computadores: peculiaridades da formação do vínculo**. São Paulo: Saraiva, 2001.

7. BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: 2018, Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 22 maio 2025.

8. GOOGLE**. Política de Privacidade**. Disponível em: Política de Privacidade – Privacidade & Termos – Google. Acesso em: 25 maio 2025.

9. META. **Política de Privacidade da Meta — Como a Meta coleta e usa os dados do usuário | Central de Privacidade,** Disponível em: https://www.facebook.com/privacy/policy. Acesso em: 24 maio 2025.

10. TIKTOK. **Política de Privacidade** | TikTok. Disponível em: https://www.tiktok.com/legal/page/row/privacy-policy/pt. Acesso em: 27 maio 2025.

11. X CORP. **Política de Privacidade**. Disponível em: https://privacy.x.com/pt . Acesso em: 27 maio 2025.

12. HALE, Durval. **Lei Geral de Proteção de Dados: Manual de Compliance.** Brasília/DF: Instituto de Registro de Títulos e Documentos e de Pessoa Jurídica do Brasil, 2021.

13. BRASIL. Autoridade Nacional de Proteção de Dados – **ANPD. Saiba como fiscalizamos**. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/fiscalizacao-2/saiba-como_fisalizamos?_authenticator=b05dbbec15247ce4c8b7065d588ef945f6d4d340. Acesso em: 21 maio 2025.

14. BRASIL. Autoridade Nacional de Proteção de Dados – ANPD. **ANPD abre processo sancionador e emite determinações ao TikTok.** Publicado em 04/11/2024. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-abre-processo-sancionador-e-emite-determinacoes-ao-tiktok. Acesso em: 21 maio 2025.

15. MARANHÃO. **Tribunal de Justiça do Estado do Maranhão – TJMA. Portal do Poder Judiciário do Estado do Maranhão.** Disponível em: https://www.tjma.jus.br/midia/portal/noticia/516274/justica-condena-apple-e-google-por-violarem-a-protecao-de-dados-pessoais. Acesso em: 24 maio 2025.