Revista ARACÊ
ISSN: 2358-2472

SURVEILLANCE CAPITALISM, FUNDAMENTAL RIGHTS AND THE CONSTITUTIONAL PROTECTION OF DATA PROTECTION IN BRAZIL

CAPITALISMO DE VIGILÂNCIA, DIREITOS FUNDAMENTAIS E A TUTELA CONSTITUCIONAL DA PROTEÇÃO DE DADOS NO BRASIL

CAPITALISMO DE VIGILANCIA, DERECHOS FUNDAMENTALES Y LA PROTECCIÓN CONSTITUCIONAL DE LA PROTECCIÓN DE DATOS EN BRASIL

https://doi.org/10.56238/arev7n7-253

Date of submission: 06/21/2025 **Publication Date:** 07/21/2025

Vinícius Teixeira Bressan[1] and Jailson de Souza Araujo[2]

ABSTRACT

This article is intended to analyze, from a comprehensive perspective, the constitutional protection of data protection in Brazil. It seeks to demonstrate that the popularization of the internet has been permeated by the constantly monitored and camouflaged of users, which not only violates the right to privacy but also harms the right to self-determination. Based on a hypothetical-deductive approach based on the method of bibliographic review, the study deals with the insufficiency of the legislative protection prior to the enactment of Law No. 13,709/2018, and the factual conjunctures that made it necessary to have a specific standardization of the matter. In addition, under the focus of the constitutionalization of civil law, the main protection mechanisms created by the General Data Protection Law are outlined, as well as the means of monitoring and punishing any incidents involving the processing of personal data. Based on the analysis undertaken, it is demonstrated that the LGPD is based on the expansionist conception of personal data, and that it is an instrument capable of safeguarding intimacy in the virtual environment and curbing the stigmatization of the user of the networks. Finally, it is the central role of the National Data Protection Agency of the Judiciary in the application of sanctions to processing agents, with a view to the realization of this important fundamental right, which is directly linked to the safeguarding of Human Dignity.

Keywords: Surveillance Capitalism. Digital Law. General Law for the Protection of Personal Data. New Information and Communication Technologies. Data Privacy.

[1] Lawyer and Municipal Attorney of Matinhos/PR. Graduated in law from the Federal University of Paraná (UFPR). Specialist in Applied Law from the School of Magistrates of the State of Paraná (EMAP-PR). Specialist in Bids and Administrative Contracts from the Pontifical Catholic University of Paraná (PUC-PR). Master's student in Law at the International University Center (PPGD-UNINTER), under the guidance of Professor Daniel Ferreira.
E-mail: viniciustbressan@gmail.com.

[2] Dr. in Economic and Socio-Environmental Law from PUC/PR. Permanent Professor of the Master's Degree in Law at the International University Center – PPGD-UNINTER. Lawyer.
E-mail: araujoadv@yahoo.com.br.

RESUMO
Este artigo pretende analisar, sob uma perspectiva compreensiva, a proteção constitucional da proteção de dados no Brasil. Busca demonstrar que a popularização da internet tem sido permeada pela constante vigilância e camuflagem dos usuários, o que não só viola o direito à privacidade como também fere o direito à autodeterminação. A partir de uma abordagem hipotético-dedutiva, com base no método de revisão bibliográfica, o estudo aborda a insuficiência da proteção legislativa anterior à promulgação da Lei nº 13.709/2018 e as conjunturas fáticas que tornaram necessária uma normatização específica da matéria. Além disso, sob o enfoque da constitucionalização do direito civil, são delineados os principais mecanismos de proteção criados pela Lei Geral de Proteção de Dados, bem como as formas de fiscalização e punição de eventuais incidentes envolvendo o tratamento de dados pessoais. Com base na análise empreendida, demonstra-se que a LGPD se fundamenta na concepção expansionista de dados pessoais, sendo um instrumento capaz de resguardar a intimidade no ambiente virtual e coibir a estigmatização do usuário das redes. Por fim, destaca-se o papel central da Agência Nacional de Proteção de Dados do Poder Judiciário na aplicação de sanções aos agentes de tratamento, visando à efetivação desse importante direito fundamental, diretamente vinculado à salvaguarda da Dignidade da Pessoa Humana.

Palavras-chave: Capitalismo de Vigilância. Direito Digital. Lei Geral de Proteção de Dados Pessoais. Novas Tecnologias da Informação e Comunicação. Privacidade de Dados.

RESUMEN
Este artículo analiza, desde una perspectiva integral, la protección constitucional de la protección de datos en Brasil. Busca demostrar que la popularización de internet se ha visto afectada por la constante vigilancia y ocultación de los usuarios, lo que no solo viola el derecho a la privacidad, sino que también perjudica el derecho a la autodeterminación. Con un enfoque hipotético-deductivo basado en la revisión bibliográfica, el estudio aborda la insuficiencia de la protección legislativa antes de la promulgación de la Ley n.º 13.709/2018 y las circunstancias fácticas que hicieron necesaria una estandarización específica en la materia. Además, bajo el enfoque de la constitucionalización del derecho civil, se describen los principales mecanismos de protección creados por la Ley General de Protección de Datos, así como los medios para monitorear y sancionar cualquier incidente relacionado con el tratamiento de datos personales. Con base en el análisis realizado, se demuestra que la LGPD se basa en una concepción expansionista de los datos personales y que es un instrumento capaz de salvaguardar la intimidad en el entorno virtual y frenar la estigmatización del usuario de las redes. Finalmente, se destaca el papel central de la Agencia Nacional de Protección de Datos del Poder Judicial en la aplicación de sanciones a los responsables del tratamiento, con miras a la realización de este importante derecho fundamental, directamente vinculado a la protección de la dignidad humana.

Palabras clave: Capitalismo de vigilancia. Derecho digital. Ley General de Protección de Datos Personales. Nuevas Tecnologías de la Información y la Comunicación. Privacidad de datos.

INTRODUCTION

This article deals with the constitutional protection of data protection in Brazil, focusing on the factual contingencies that gave rise to the specific regulation of the matter, and the insufficiency of the legislative protection that preceded the enactment of Law No. 13,709/2018 - and the subsequent enunciation of a specific constitutional provision on the subject. In view of this, the study aims to demonstrate the main protection instruments governed by the General Data Protection Law (LGPD), and its concrete importance in safeguarding Human Dignity in the virtual context.

In addition, the reflection brought permeates the role of the National Data Protection Authority (ANPD) in the regulation of data processing activities and in the application of sanctions to processing agents, as well as the importance of an energetic action by the Judiciary in civil liability related to data breaches, as a way to deter irregular behavior by processing agents.

The work is based on the hypothetical-deductive method, and was developed through a literature review – notably, of current scientific articles that have been published on the subject. Through the study, it is intended to outline a comprehensive analysis of the subject, which covers from the normative and factual antecedents that gave rise to the enactment of the LGPD [and the constitutional enunciation of the right to the protection of personal data], the gains resulting from it in terms of the realization of fundamental rights, and the need for effective accountability of those responsible for the inappropriate processing of personal data, so that the legal and constitutional precepts are effectively materialized by the processing agents.

In this regard, we seek to contextualize the reader as a scenario of digital hyper-surveillance of users in the virtual context, which is one of the main marks of the practices of today's capitalism, surveillance capitalism - a term used by Lucca and Martins (2024) to refer to promotional campaigns promoted through the massive collection of data on websites. This is the hidden face of many of the facilities arising from the popularization of the internet, which gave rise to the enactment of Law No. 13,709/2018 and Constitutional Amendment No. 115, of February 10, 2022, which included item LXXIX to article 5 of the Federal Constitution, safeguarding the protection of personal data as an autonomous fundamental right.

In addition, some of the legal initiatives prior to the General Data Protection Law (LGPD) that safeguarded, albeit timidly, the protection of internet users' data in Brazil are addressed, focusing on the need to enact a specific law to deal with the subject. Below, a general overview of the protection provided by the LGPD is outlined, which is permeated by the analysis of the main protection mechanisms aimed at safeguarding the rights of personal data subjects in Brazil, their scope, the centrality of the user's consent and the nuances of the hypothesis of data processing based on legitimate interest - all under the focus of the constitutionalization of the right and the role of the General Law in the promotion of fundamental rights. Further, practical examples of the application of data protection rules to the scope of labor relations are set out, in order to safeguard that the article is not limited to the purely theoretical level.

In the last chapter, the sanctioning discipline set forth by Law No. 13,709/2018 is addressed. To this end, it discusses the role of the National Data Protection Authority (ANPD) in the application of sanctions to processing agents and the main contours of civil liability for violation of data protection rules, from the perspective of facilitating the defense of the data subject and the importance of effective punishment of irregularities committed in the processing of personal data, as a means of compelling processing agents to comply with existing standards.

DATA MONITORING, PROFILING, AND DIGITAL VULNERABILITY IN SURVEILLANCE CAPITALISM

Access to the internet has been recognized as a human right by the UN, as it enables the broad exercise of freedom of expression. Safeguarding this requires, however, the creation of mechanisms capable of making this fundamental right compatible with the protection of intimacy, private life, honor, image, and the protection of personal data (Ribeiro, 2022), otherwise digital platforms will become instruments of human rights violations.

It is undeniable that technological advancement is capable of providing degrees of comfort that were previously unimaginable. However, it is a fact that many of the facilities that are currently attributed to artificial intelligence and modern algorithms are the result of the combination of [often sensitive] data, which allow computer devices to trace patterns of behavior, interests and trends of the user. The manipulation of personal information entails a risk, almost always hidden, of data leakage and violation of privacy and honor, which requires assertive legal protection, which is capable of making technological development compatible with the guarantee of fundamental rights (Andréa, Arquite, and Camargo, 2020).

We live in the midst of surveillance capitalism - a term used by Lucca and Martins (2024) to refer to promotional campaigns promoted through the massive collection of data on websites. This is done for the purpose of tracing personality and consumption profiles, and inducing behaviors – especially for greater effectiveness in commercial strategies. In this context, the availability of information about consumer preferences has become an important business asset (Oliveira, 2018). The so-called behavioral marketing is an assertive advertising method, which is based on the formation of the individual consumption profile of each user of the network, and is obtained through the combination of data collected during interactions carried out in the virtual sphere (Verbicaro and Calandrini, 2022).

The collection of data occurs through access to free applications, acting on social networks, conducting research and virtual registrations or, in the field of illegality, through spam and spyware (Cavet and Faleiros Júnior, 2024). This collection can even transcend the exclusively virtual scope, such as the company that manages a subway line in São Paulo that, in 2018, installed sensors to collect biometric data and passengers' reactions in relation to the advertisements displayed, for the purpose of creating psychic patterns related to the type of advertisement and its content - which, that is, it gave rise to the filing of a public civil action, in which the preliminary withdrawal of the equipment was ordered (Calabrich, 2020).

Once accumulated, the data is processed and converted into behavioral patterns and, later, it is sold to the one among the interested parties who is willing to pay a higher monetary amount for the information - a fact that gives rise to true objectification of the human being, and their experiences (Martins and Longhi, 2022).

Through pre-defined command sequences, computer programs are able to interpret habits and records to predict behaviors and trends, and to create a virtual representation of the human person. Based on this, not only the ads, but also the information that will be made available to the user will be dictated by this parameter of preferences absorbed by artificial intelligence. This, unequivocally, undermines the formation of a critical sense of the individual, and the exercise of the right to informational self-determination of those who use the internet (Lucca and Martins, 2024), a fact that arouses special concern when it comes to young people, who tend [or at least would tend] to substantially change their convictions with the acquisition of maturity.

In other words, the targeting of information and advertisements based on behavioral marketing ends up interfering both in the formation of the individual's critical thinking and in the decisions made in the consumer market, which are guided by a digital reflection of their personality that is combined with neuroscientific techniques of persuasion - which can, therefore, in many cases, to prevent citizens from making choices in a truly free and informed way (relegating human beings to the role of a mere supporting player in their decision-making processes). Also because it involves an aggressive invasion of the user's privacy, the use of profiling to unconsciously influence consumers to purchase products and services requires special concern in the current consumer society, which is permeated by commercial transactions that are predominantly not aimed at meeting personal needs, but at meeting emotional anxieties and superfluous desires that are typical of the information age (Cavet and Faleiros Júnior, 2024).

In short, nowadays, the combination of information through algorithms shapes consumption preferences, the type of information that will be presented during electronic navigation and the circle of people to be connected in the virtual environment, which is only possible due to the permanent collection of a high volume of data, and the combination of them. so that they can be used in the most varied commercial desiderata. The availability of data has acquired special commercial value in the mainstays of surveillance capitalism that companies such as Meta and Microsoft, whose operations are centered on the collection and processing of personal data, boast enormous commercial value (Búrigo and Carloto, 2023).

Notwithstanding the high market value of personal data, it is a fact that users hardly understand the consequences of providing data, and the risks associated with storing and handling them. An example of this is the study developed by the psychology department of the University of Cambridge, in which it was inferred that 4/5 of its participants would give access to personal information about themselves and their friends, including indicating their respective addresses, in exchange for the reduced value of one dollar (Cavet and Faleiros Júnior, 2024).

The result is, however, understandable, since digital profiling mechanisms involve a very nebulous reality, in which economic agents [and the State itself] hold ample information about individuals, and they are unaware of the operations carried out based on their data. An extreme but paradigmatic example of how harmful the effects of digital hyper-surveillance can be was the development of a system by the Chinese government in 2018 to classify its citizens according to their behaviors and, based on the score assigned, prohibit the purchase of plane and train tickets – which allowed more than twenty million trips to be barred by 2020 (Calabrich, 2020).

In view of this, it is noted that the advancement of technology has not only provided an expansion of access to information and the reconfiguration of social and work relations, but has also eliminated communication barriers, diluted the boundaries between domestic and work space, and required the resignification of the right to intimacy and privacy, for example (Sturmer and Miranda, 2023).

Considering the high potential for disseminating information in virtual media, the protection of privacy, image and intimacy is now immediately linked to the protection of personal data – especially sensitive data. These are the ones that are pertinent to the particularities of a given person, which involve their political, religious, and philosophical preferences, as well as issues related to health, sexual preference, which are topics directly linked to the private sphere of the human being (Andréa, Arquite, and Camargo, 2020).

Reinforcing the special importance of data protection, it must be considered that, in addition to its relevance in terms of guaranteeing fundamental rights, the interests of the State and companies do not always converge with those of each person, at least in the individual sense (Calabrich, 2020), which has also made the standardization of data processing in Brazil urgent.

The need for specific regulation of the matter, with the establishment of requirements for information security standards, is evidenced by the various examples of incidents involving data leaks that occurred in the very near past.

In 2016, there was a leak of data related to blood donors from Australia, which culminated in the publicity of internal records affecting people with risky sexual behavior. In 2017, it was discovered that an erotic equipment developed by a Canadian company, which connected to the cell phone, sent real-time data to the developer about how it was used (Lucca and Martins, 2024).

Likewise, in 2020, several patient data leaks were recorded from the Unified Health System, which intensified discussions about the need to improve the means of data protection of the Public Authorities (Cerqueira, 2022).

Another data leak scandal involved the provision of information of millions of users of the social network Facebook to the company Cambridge Analytica, starting in 2014 - a fact that may have been crucial to influence voters, based on the establishment of their profiles and preferences, and decisive for the election of candidate Donald Trump, in the United States of America, in 2016 (Suzin and Aguiar, 2023).

An event that, although it does not constitute a data incident, provokes reflections and highlights the importance of clear rules that govern data protection was the prediction of the swine flu epidemic in the United States of America by the engineers of the Google search platform, based on the combination of search patterns carried out by users, and in user monitoring (Lucca and Martins, 2024). Without adequate standardization of the matter, the finding could have been passed on, obviously in secret, to the pharmaceutical industry, which could stimulate opportunistic behaviors such as the increase in the price of medicines, thus making it difficult to control the disease (Martins and Longhi, 2022).

Reinforcing the importance of data protection protection, it should be considered that algorithms, as sequences of commands that must be executed in the processing of information, are not capable of discerning inappropriate or discriminatory parameters, nor of accurately understanding contexts - which is exemplified by the robot developed by Microsoft to interact with social network users, which had to be taken down quickly, as it normalized the prejudiced behavior of users (Calabrich, 2020).

It must be recognized that, before the enactment of Law No. 13,709/2018, other laws safeguarded some safeguard, albeit tangentially and generically, for the data of internet users. In this sense, for example, the Consumer Protection Code already regulated consumer databases, and Law No. 12,414/11 (Positive Registry Law) already regulated the processing of socioeconomic data for the purpose of granting credit, stating the operator's duty to obtain the consent of the holder prior to the transfer of data to third parties, and prohibiting the collection of information disconnected with the intended purpose, as well as the use of this for purposes other than that passed on to the holder. Likewise, the so-called Civil Rights Framework for the Internet (Law No. 12,965/2014) regulated, in 2014, the compatibility of the exercise of freedom of expression in digital media with the rights of other internet users and, in the criminal sphere, Law No. 12,737 of 2012 criminalized the non-consensual invasion of electronic devices, after the leak of intimate photographs of actress Carolina Dieckmann (Andréa, Arquite and Camargo, 2020).

With technological evolution, data processing has become increasingly complex and susceptible to the violation of fundamental rights, which required specific regulation of the subject. This happened with the approval of the General Law for the Protection of Personal Data (Law No. 13,709/2018), which protects the collection and processing of personal data by individuals and legal entities, and which is the result of intense debates in the National Congress, which were permeated by the participation of representatives of the various interested sectors (Andréa, Arquite, and Camargo, 2020).

Another important step in the protection of personal data was the approval of Constitutional Amendment No. 115, of February 10, 2022, which included item LXXIX to article 5 of the Federal Constitution, safeguarding the protection of personal data as an autonomous fundamental right, conferring exclusive legislative competence on the Union to deal with the issue and attributing to it the role of organizing and supervising the protection and processing of data (Cardoso, 2023).

In short, until the enactment of the LGPD and the approval of Constitutional Amendment No. 115, of February 10, 2022, "the right to the protection of personal data was seen as an unfolding of the right to intimacy (...). But, despite conceiving this right, it was not given adequate treatment, which gave rise to gaps and misrepresentations" (Suzin and Aguiar, 2023).

It is that, in view of the realization that personal data began to be massively collected in the midst of the popularization of the internet, initially, it was necessary to safeguard the right of its holder to consent [or not] to the processing of their data, as a way of realizing their rights to freedom and privacy. After this, it was observed that mere consent was not enough, and that a more specific protection of data operations would be necessary, in order to safeguard the existence of minimum standards to be followed in the processing of personal information (Suzin and Aguiar, 2023).

Having fulfilled the desideratum of clarifying the risks of data processing in the midst of surveillance capitalism, and the factual and legislative context that preceded the enactment of Law No. 13,709/2018 (General Data Protection Law – LGPD), it is up to us to briefly analyze the general lines of the protection of data protection existing in Brazil.

LGPD AND THE PROTECTION OF DATA PROTECTION IN BRAZIL

It is known that the protection of privacy is not a recent concern, or even exclusive to the information society, as there are articles debating the importance of its protection in the early 1980s. This is a fundamental right consolidated by the current constitutional order, which is precisely the central point of the discipline carried out by the General Law for the Protection of Personal Data (LGPD), which gravitates around the right of citizens to decide on the use [or not] of their data in operations, and on the purposes that may be achieved by the authorized processing (Cerqueira, 2022).

The Brazilian General Data Protection Law is strongly inspired by the General Data Protection Regulation enacted by the European Parliament in 2018, which set strict parameters for data processing activities, and strong penalties for cases of non-compliance (Búrigo and Carloto, 2023).

The influence of the European Union rules was not limited to the legislative technique, since, in parallel with the need for standardization already outlined above, the requirement set out in the General Regulation for European companies, to contract only with foreign firms whose country had adequate legal protection for data processing, required Brazil to regulate the matter, under penalty of their companies not being able to maintain commercial relations with European companies (Oliveira, 2018).

Law No. 13,709/2018 regulated all personal data processing activities in the country, including those carried out by the Government and those carried out on a non-profit basis. To this end, in addition to enunciating rules to be observed in data operations, it listed principles that should guide its application [and all rules that deal with the matter, whether they are other laws or infra-legal acts]. Such a principle is based on the ideal of protecting the privacy of the data subject, through the legal protection of information capable of allowing, in a singular or associated way, the identification of the natural person (Cardoso, 2023).

Therefore, the LGPD does not exclusively protect sensitive data, since it is based on the expansionist conception of personal data (Oliveira, 2018), which encompasses all those that allow the identification of the person directly and, also, those that, when combined, also need the identity of the holder, as mentioned above. For example, data on purchase, browsing data, and information on the individual's movement may not be significant if considered in isolation, but, combined, they allow the perfect identification of the sexual, philosophical, and political preferences of the internet user (Lucca and Martins, 2024), which is why they are covered by the LGPD.

Regarding the principle adopted by Law No. 13,709/18, the "principle of finality (...) links the processing to a specific purpose (...), its modification is prohibited, as a rule, without the collection of new consent (...), and the principle of necessity, which allows the processing only of data essential to achieve the purpose (...)" (Oliveira, 2018). There is also an implicit principle, which arises from the confluence of the LGPD's provisions on the need to neutralize risks of harm, which is the precautionary principle, which imposes a positive duty on processing agents, who are responsible for developing incident prevention routines (Martins and Longhi, 2022).

Therefore, a practice similar to the processing of data without prior consent (not supported by the presence of the requirements that exempt it, obviously), is the deviation of the purpose of the data processing authorized by the user, since the operations must meet the purpose foreshadowed to the holder of the information, and that the use for other purposes constitutes an illegal act (Cavet and Faleiros Júnior, 2024).

By supporting data subjects, Law No. 13,709/18 conferred on them several rights, such as knowledge about data operations, anonymization of information, and correction of erroneous information, for example. In addition, it attributed to the controlling agent, understood as the data operator how the processing will take place, a duty of transparency regarding the method used, the scope of the operations, the form of systematization, the main impacts and risks of data handling - which must, as a rule, be clarified to the requesting user and, unrestrictedly, to the National Data Protection Authority (ANPD) (Calabrich, 2020).

Despite the centrality of consent in the field of data protection, after the second public hearing held in the National Congress during the legislative process of the LGPD, the legitimate interest for data processing was included among the authorizing hypotheses, in response to the desires for flexibility of data agents, who militated the impossibility of obtaining user consent in each processing operation (Verbicaro and Calandrini, 2022).

By legal requirement, the operation must be carried out from a concrete situation, directed to a legitimate interest, and prioritize respecting the legitimate expectations of the data subject. As "legitimate interest" is a vague and indeterminate concept, its invocation requires a certain reasonableness from the agent, under penalty of degrading the protection of fundamental rights of the respective holder (Oliveira, 2018). As it is a hypothesis of processing that does not require the consent of the data subject, it deserves special caution from legal operators, who are responsible for enunciating interpretative parameters capable of reconciling the ideal of plasticity intended by entrepreneurs with the duty of obedience to the fundamental rights of the data subject.

In addition to complying with the legal requirements, as inevitable, the performance of the processing agent must be guided by the principle of purpose and necessity, which require, respectively, that the operation justified by legitimate interest be carried out based on reasons aligned with the legal system, and that the data be summarized to the minimum necessary – always observing the right to information that the interested party has, and the need to enunciate concrete justifications to support the operation (Verbicaro and Calandrini, 2022).

It is noteworthy that, although the LGPD does not exclusively regulate operations involving sensitive data, given the potential to support stigma, discrimination, and social segregation – which can sometimes give rise to physical violence and defamatory campaigns – this special class of information, of a clearly existential nature, enjoys [and, it must be said, needs to enjoy] special legislative protection (Lucca and Martins, 2024).

It is worth remembering, at this point, that after the Second World War, the legal systems were resignified under the prism of the recognition of the normative force of the Constitution, so that all the norms of the legal system became materially subordinated to the fulfillment of their central values, especially the Dignity of the Human and the rights related to it (Siqueira Júnior, 2011).

Inspired by the ideals of protection and promotion of fundamental rights, Law No. 13,709/2018 safeguarded the protection of personal data both from the perspective of privacy and the prohibition of data processing for discriminatory and unlawful purposes, which may cause the exclusion or harm the enjoyment of rights inherent to the human condition, always aiming at the achievement of material equality (Lucca and Martins, 2024).

Illustrating the need to protect personal data from the perspective of non-discrimination, in 2018, the company Decolar had to be sanctioned in a millionaire figure for the practice of geopricing, which consisted of differentiating the prices of airline tickets according to the consumer's location. Similarly, Amazon's staffing system favored hiring men over women. In addition, Google Photos' recognition algorithm identified black people as gorillas, and a system developed to help the U.S. judiciary assess the chances of criminal recidivism tended to predict almost twice as much risk when it came to black people, and consider white people as at low risk of reoffending (Calabrich, 2020).

In view of the direct link between sensitive data and the realization of fundamental rights, the legislator chose to condition its processing to specific consent, highlighted and aimed at a specific desideratum previously declared, which will only not be required in exceptional situations, such as the development of public policies, the prevention of fraud and threats, and the use of biometrics. Likewise, the LGPD allowed health data to be manipulated for studies, but required its anonymization, compliance with the rules of the Code of Medical Ethics, the maintenance of information in a restricted environment, and prohibited the sharing of health data for profit to other processing agents (Lucca and Martins, 2024).

Another issue that deserves to be highlighted is the fact that, although the original wording of Law No. 13,709/18 provided for the possibility of review of automated decisions by natural persons, this provision was suppressed by Provisional Measure No. 869/2018, later converted into Law No. 13,853/2019, which made it possible for even an eventual review to be robotized. This was based on the premise that new business models could be made unfeasible by the need for personnel to review algorithmic decisions, and that there would be substantial impacts on the risk analysis inherent to credit operations. On the other hand, in view of the legislative change, the LGPD now requires the controller to provide clear information about the criteria used in the automated decision and that, if it cannot do so to protect industrial secrecy, the National Data Protection Authority, which will be discussed below, may audit the algorithm to verify the existence or not of discriminatory criteria, which are prohibited by law (Calabrich, 2020).

In addition, despite the apparent divergence between the legal discipline of data processing enunciated by the LGPD and the Civil Rights Framework for the Internet, it is a fact that the latter only disciplined the processing of data in a subtle way, being insufficient to regulate the matter, and that, under the aegis of the legislative specialty, in the event of a normative conflict, the concrete situation must be protected by that rule. In any case, it will be necessary to seek, in most cases, a combined application of both, in order to safeguard greater protection for the user, insofar as article 64 of the LGPD states that its content does not exclude the protective framework established by other national and international rules that deal with the subject (Oliveira, 2018).

At the same time, it must be recognized that technological advances have allowed the State to know in detail the urgencies of the population, and to develop more assertive public policies, in addition to modernizing the urban mobility system (Oliveira, 2018), which amounts to nothing more than the fulfillment of the duty of efficiency incumbent on the Public Power by the administrative reform of 1998, which marked the transition from the bureaucratic to the managerial model, oriented to results (Leal Júnior and Penha, 2022). Access to information itself, in fact, allowed a true resignification of the constitutional principle of publicity, which is no longer limited to the publication of data in official gazettes (Neves, 2018).

In any case, the General Data Protection Law has been frequently invoked by public agencies to justify refusals to access public data – a fact that is not compatible with the current constitutional system, nor with the dictates of Law No. 12,527/2011 (Access to Information Law, or LIA) (Cerqueira, 2022).

In this regard, it should be considered that access to information is one of the bases of participatory democracy, and that it is the means safeguarded by the citizen to evaluate the role played by the State and the forms of application of public resources, to claim rights and to participate in the direction of the Public Administration (Deienno and Santos, 2014, p.17).

The applicability of the LGPD to the public sector is unequivocal and indisputable. However, this does not mean that requests for access should [or even can] be rejected in honor of the protection of data protection, since there is a relationship of complementarity - and not opposition - between the LGPD and the LIA, insofar as they protect, respectively, constitutional rights of access to information, and to privacy and data protection, Thus, it is up to public agencies to establish efficient data classification mechanisms that allow a harmonious protection of both. It should be said: only information of a personal nature capable of identifying its holder is protected from disclosure by the LGPD, and there is no reason why those that do not concern the identification of taxpayers, property data, their private life and intimacy [and, as a rule, extensively, public servants and political agents] should not be disclosed by the State - provided, obviously, there is no incidence of any of the hypotheses of secrecy enunciated by the LIA. (Cerqueira, 2022).

Having presented the main protection mechanisms contemplated by the LGPD to safeguard the rights of data subjects in Brazil, in order to illustrate the importance of the LGPD, especially so that this article is not limited to purely theoretical issues that could often be observed through the reading of Law No. 13,709/18, it is now stated, In the following paragraphs, some practical examples of the application of data protection rules to the scope of employment relationships.

As the labor field involves the periodic collection and processing of worker data, it is easy to infer that the LGPD radiates its effects on the protection of workers' rights, whether public or private. In this regard, the management of data related to the employee's health is especially important, especially certificates and information related to the professional's medical condition. On the subject, mention is made of the conviction for moral damages imposed in 2020 on the Sanitation Company of Minas Gerais by the Regional Labor Court of the 03rd Region, due to the permission of unauthorized people to access an employee's health information, through the internal computerized system. Another clear example of the importance of protecting the worker's sensitive information was the annulment, in 2019, of a clause in a collective bargaining agreement that provided for the obligation to indicate an ICD for the purpose of compensating for absences, under the premise that the inclusion of this information can only take place at the initiative of the holder, including under penalty of violation of the Code of Medical Ethics (Búrigo and Carloto, 2023).

Likewise, the protection of data protection and intimacy that was advocated by the LGPD radiates direct effects on labor relations permeated by telework. As fixed-time employment contracts require the payment of additional overtime or the institution of compensatory time off for excess hours, the use of employee surveillance applications has been frequent. Some of them involve monitoring screens, reading WhatsApp messages and social networks, geographic tracking, capturing images and sounds, for example – a fact that is aggravated, in most cases, by the absence of prior awareness of the interested party, and by the fragility of any consent granted in the work environment, which is marked by marked asymmetry. Under the aegis of the LGPD, it is unthinkable that the employer can employ many of these resources, especially the monitoring of conversations and images through webcam, since the hypothesis of treatment to guarantee the security of the holder is focused on biometric authentication, and that fraud prevention must presuppose prior evidence capable of relativizing intimacy. In fact, even geolocation monitoring should be used sparingly, as it is forbidden for the employer to draw preference profiles or the employee's habits outside the working day through this type of operation (Hentges and Coimbra, 2022).

In the same vein, the consent of the data subject acquires special difficulty in the scope of labor law, which is largely marked by the asymmetry between employee and employer. For this reason, it is necessary that valid consent must be conditioned to the presence of ostensible information regarding the possibility of refusal, its possible consequences and, above all, the purpose intended with the data processing, the scope of collection, and the possibility of revoking consent at any time (Búrigo and Carloto, 2023).

As algorithms have been used even in the analysis of resumes and in the selection of employees, it is necessary to ensure that data programming does not give rise to any form of discrimination - a practice prohibited by the LGPD, which, as exposed, prohibits any processing of data with an illicit or discriminatory bias, and also by Law No. 9,029/95, which prohibits the limitation of access to work for reasons of race, sex, individual preferences, age and the like. To this end, it is understood that the data protection rules contained in the LGPD will only be complied with if the computerized systems are programmed to exclusively investigate the candidate's professional aptitude, regardless of the analysis of data outside this desideratum, such as gender, marital status or personal positions of the interested party. At the same time, it seems essential to develop routines for periodic checking of the profiles that have been selected by electronic systems, so that it can be inferred whether, in practice, the algorithm is not adopting segregated parameters (Sturmer and Miranda, 2023).

Having exhausted the scope of this topic, we now present some brief notes regarding the sanctioning mechanisms developed by the LGPD, and the rules of civil liability for violation of duties related to the processing of data contained therein.

LGPD AND THE ACCOUNTABILITY MECHANISMS FOR VIOLATION OF DATA PROCESSING RULES

In view of the constitutionalization of administrative law, any sanction for non-compliance with duties in data operations must be preceded by an administrative proceeding of a sanctioning nature permeated by adversarial proceedings and ample defense. In addition, as required by the LGPD, any penalty must observe criteria such as the seriousness of the fact, the existence or not of bad faith, and the agent's recidivism (Andréa, Arquite, and Camargo, 2020).

According to Law No. 13,709/2018, it is up to the National Data Protection Authority (ANPD), in addition to regulating data processing activities under the bias of minimal intervention and signing understandings regarding the interpretation of the LGPD, to apply sanctions in the event of non-compliance with duties by the processing agent. Although the ANPD cannot, due to a presidential veto of Law No. 13,853/2019, suspend the activity of processing personal data in the event of irregularities being found, it can apply warning penalties, a fine of up to 2.00% of the company's revenue, a daily fine for readjustment (limited, in any case, to fifty million reais), of publicizing the irregularity found, of the elimination of data related to the irregularity and of blocking these regularization (Calabrich, 2020).

It is worth mentioning that the National Data Protection Authority, with a regulatory and sanctioning role, only entered into effective external activity in 2021, as an integral body of the Federal Direct Administration structure – therefore, without technical and financial independence. It was only with the conversion of Provisional Measure No. 1,124/2022 into Law No. 14,460/2022 that the ANPD began to act autonomously, as a special agency (Cardoso, 2023).

This autarchy has, therefore, the role of "acting preventively in the construction of a rational and permanent dialogue with economic agents and civil society, but also, in an energetic and effective way, repressing illicit conduct in an exemplary manner" (Verbicaro and Calandrini, 2022).

It should be considered that the ANPD has a crucial role in the supervision of data operations based on legitimate interest - which, as it is a concept endowed with a high degree of abstraction, requires proactive inspection action by the Public Power. By provision of paragraph 3 of article 10 of the LGPD, the agency may request a data protection impact report due to the use of legitimate interest as a processing hypothesis (which, it should be said, has proven to be quite common). As this authorizing assumption does not require consent, and data processing is not very accessible [and even understandable] to users, it can be seen that operations based on legitimate interest are based on the data subject's confidence in relation to the lawfulness of the processing agents' actions – which requires, for the purposes of supporting the legitimate expectations of the data subject, the development of efficient ANPD control mechanisms, whether through inspection, education, or even sanctioning, always aimed at avoiding abuses and the compromise of the national data policy (Verbicaro and Calandrini, 2022).

As for civil liability, it can be seen that, by regulating the issue, Law No. 13,709/2018 was not limited to protecting the compensation of damages, since it also foreshadowed the need to prevent incidents involving data processing. In this sense, article 6, X, of the LGPD linked issues inherent to the agent's accountability to the accountability to the user regarding the mechanisms used to protect personal data and the demonstration of their effectiveness. Items VII and VIII of the same article, in turn, govern the need to develop routines capable of preventing data incidents, and to adopt methods capable of protecting data from unauthorized access, loss and improper alteration. Articles 42 to 45, in a complementary way, regulate the duty to indemnify damages suffered by the data subject due to failures in data operations – which usually have serious consequences for the user's image and privacy (Ribeiro, 2022).

Under the aegis of article 927, Sole Paragraph of the Civil Code, which affirmed the adoption of the risk theory in Brazil, article 42 of the LGPD should be interpreted as enunciating strict liability for damages caused in data processing operations, given that the performance of the data controller and operator, by nature, exposes the rights of the holders to risks. It is unthinkable, in this context, that due to the mention that the obligation to indemnify would arise from damage caused by violation of the legislation that deals with data protection, the legislator has established a hypothesis of subjective liability (Martins and Longhi, 2022) - which would be extremely pernicious for excessively violating the data subject in a context of informational asymmetry and enormous opacity of personal data operations.

Despite the fact that there is no reproduction of article 927, Sole Paragraph of the Civil Code in the LGPD, it is a fact that the protection conferred by the civil legislator has already sufficiently stated that the agent whose performance is capable of putting the rights of third parties at risk must repair damages regardless of the investigation of guilt, or evaluation of the level of compliance with the duty of care. In other words, although the LGPD has not expressly defined the civil liability regime applicable within its normative scope, a systematic interpretation of civil legislation allows us to infer the hypothesis of data processing attracts the objective liability of the agent, since the nature of the activity exposes the data subject to risks of damage (Cardoso, 2022).

Especially because, it is worth repeating, the damages arising from security incidents are intrinsic to data operations and, therefore, the risks arising from them are also intrinsic. It should be considered, at this point, that from the perspective of strict liability, the processing agent will be encouraged to invest in stricter security parameters to avoid incidents and, therefore, the payment of compensation. The opposite is also true. In the event of subjective liability, the victim will end up having to internalize, as a rule, the damages arising from the processing of data carried out by third parties (which, it is worth repeating, is a highly profitable activity for suppliers), which will lead to lower levels of care by the data operator. It cannot even be suggested, at this point, that strict liability would prevent technological evolution, since this argument was raised [and overcome] in the context of the enactment of the Consumer Protection Code (Martins and Longhi, 2022).

This, in fact, will radiate effects on the vast majority of relationships entered into in the virtual sphere (provided, obviously, that its assumption of incidence is met, which is the framing of the parties in the normative concepts of supplier and consumer), so that there is no legal justification for the rule of strict liability of that subsystem to be set aside just because it is data processing.

The strong inspiration of the LGPD in the consumer code, it is worth noting, is evidenced by the rules for distributing the burden of proof. At this point, it is worth noting the existence of rules in the LGPD that impute to the controller the burden of proving the express and specific consent of the data subject (and not generic, or aimed at a purpose other than that employed by the processing agent), in the case of data operations based on consent. Also, the legal permissive for the judge to reverse the burden of proof when the holder's allegation is credible, or when the hyposufficiency or excessive difficulty in producing evidence by the interested party is evidenced, in the same way as the Consumer Protection Code – a fact that demonstrates a clear concern of the legislator to balance the unequal relationship between the processing agent and the data subject, and to avoid the adoption of abusive or unfair practices (Cardoso, 2023).

As for the subjective scope of civil liability, the LGPD provides that the controller will, as a rule, be responsible for repairing the damages caused to the user due to an incident in the data operation. The processor [provided, obviously, that it has participated directly in the data processing that generated the damage], in turn, will be jointly and severally liable with the processor when it fails to comply with the rules set forth by the controller (including the privacy policy and the organization's codes of conduct) and the data protection rules, or in the event of complying with unlawful orders from the controller - always observed, in any case, the right of recourse of the interested party against the co-respondents. In summary: the controller will be responsible for repairing the damages, either individually or jointly with the operator, depending on the case, and the operator will only be held liable when it has incurred in one of the hypotheses listed by the legislator (Cardoso, 2022).

The joint and several liability set forth by the LGPD radiates important effects to the scope of relations between entrepreneurs. A very common situation in the consumer market is the formation of contractual networks with segregation of the functions of controller and data operator, or even the sharing of information between several companies. This exchange of data requires not only that the holder be informed about the exchange of information and the purpose of this remittance, but also that the person responsible for the sending is responsible for the adequacy of the processing system of the receiving agent vis-à-vis the interested party. This requires, as inevitable, the adoption of mechanisms for joint management of risks related to information leakage, deviation of purpose of processing operations, data tampering, use of data for illicit purposes, for example, which are means of preventing a company from being penalized due to irregularities perpetrated by a business partner, even if it has been agitated correctly. It is worth remembering that, in addition to the duty to indemnify the damages suffered by the holders, irregular practices may lead to the application of administrative penalties, such as fines of up to fifty million reais and that the disclosure of the data incident may, by itself, have great repercussions in the business market, such as the loss of partners and market value. For this reason, despite the fact that the development of risk mitigation mechanisms has not been listed as a duty by the LGPD, it is highly recommended that business contracts assertively discipline not only the sharing of data, but also, at least, the contractual guarantee of compliance with data protection rules, the duty to clarify to users about the sharing of data with the business partner, the creation of mechanisms for periodic auditing of the prevention systems themselves and also those existing in the partner company, the subjection of employees to confidentiality terms, and the allocation of data in the event of a business breakdown (Andrade and Teles, 2020).

The responsibility for repairing the damage will be excluded when it is proven that the agent was not the one who carried out the data processing in question, that there was no violation of legal data protection duties, or that the risk is attributable to the victim or third parties, under the terms of article 43 of the LGPD (Brasil, 2018).

In order to be able, however, to inquire whether or not the data processing was adequate [which is one of the hypotheses exempt from liability], the parameters set out in article 44 of the same law must be observed, which involve not only compliance with legal norms, but also the provision of security standards legitimately expected by the data subject according to the way in which the data processing is carried out, the risks that reasonably arise from it and the techniques available at the time of the questioned operation. In practical terms: an operation can be considered irregular despite the faithful observance of the legislation, when it distances itself from information security standards, internal regulations, or the duty to use the best available treatment method, for example (Cardoso, 2022).

Finally, it is appropriate to recognize the existence of non-patrimonial damage in re ipsa in cases of violation of the rules for the processing of sensitive personal data, as a way to curb illegal practices. Especially in view of the potential to cause damage of an existential nature that is intrinsic to any data incident, and the need to encourage the development of routines of maximum caution in sensitive data processing operations (Lucca and Martins, 2024).

CONCLUSION

From the above, it can be inferred that the popularization of the internet has brought enormous facilities in the scope of social interactions, telecommunications, and labor relations, but it has been permeated by the digital hypervigilance of users, and by the mass collection of personal data in order to trace consumption profiles and predict behaviors - which are the distinctive mark of the so-called surveillance capitalism. In parallel with the weakening of the consumer's power of choice through neuroscientific techniques of persuasion, the creation of volatile needs inherent to the information society and the damage to informational self-determination, the normative protection of the right to private life had to be reinforced, as a way of ordering the mass processing of personal data in Brazil.

In this context, as demonstrated, the LGPD was approved to safeguard fundamental rights (especially privacy and intimacy), and to curb data operations with discriminatory, abusive purposes or capable of violating the enjoyment of rights. Its edition followed an international trend of personal data protection, amid the multiplication of serious processing incidents that have the potential to cause existential damage to their holders, and was directly influenced by the European Union's General Data Protection Regulation, which conditioned the commercial partnerships of European companies with organizations from other countries to the adequate legislative protection of the processing of personal data in the respective location.

As mentioned, the protection of personal data in Brazil is centered, to a large extent, on the consent of the data subject, and on the duty of information of the processing agent as to the extent and purpose of the operation – which should be summarized, in all cases, only to the volume of data indispensable for the intended desideratum, and stick to the specified objective. In addition, although it is not limited to safeguarding sensitive personal data, it is a fact that Law No. 13,709/2018 granted special protection to this type of information, which is directly linked to the intimate aspects of personality.

It is understood that one of the merits of the LGPD was to protect complementary interests, namely, the economic interests of the processing agents and the right to privacy and intimacy of the holder of these data. This is because, if on the one hand the massive collection of data can expose network users to risks [which justifies the legal protection of their legitimate interests], on the other hand, there is no reason to villainize the popularization of the internet, or even of data processing agents, whose performance enables the enjoyment of numerous conveniences.

In other words, what should be rejected, in any case, is the use of virtual mechanisms with the aim of making the human being hostage to his virtual representation, or even of limiting the enjoyment of rights. However, the proper processing of personal data, with the aim of improving the enjoyment of utilities, must be encouraged – and this is precisely what is aimed at the protection engendered by Law No. 13,709/2018, and the fundamental right to the proper processing of personal data that was enshrined in item LXXIX to article 5 of the Federal Constitution.

From all the above, it is conjectured that the LGPD was able to adequately regulate the processing of data in Brazil, although it is foreseen that the effective respect for the guarantees that were safeguarded to the data subject will only be obtained through a more energetic action by the ANPD, whether through inspection, educational, or sanctioning action and, also, the alignment of the Judiciary with the ideal of safeguarding energetic compensation in favor of victims of violations of the right to protection of personal data, regardless of the investigation of guilt of the processing agent. This is not only to safeguard the victim, but above all to encourage the development of more assertive and efficient routines for the protection of personal data.

Finally, it is hoped that this study will instigate new research on the matter, especially with the aim of improving the LGPD, given the need for constant adaptation of the legislation to the rapid transformations that have occurred in the virtual context and, consequently, to the new challenges to the safeguarding of fundamental rights that arise in it on a daily basis.

REFERENCES

1. Andrade, R., & Teles, B. (2020). Alguns reflexos da Lei Geral de Proteção de Dados nas relações interempresariais e as possíveis formas de gerenciamento de riscos relacionados à responsabilização solidária. Revista de Direito e as Novas Tecnologias, 8, 1-20. https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89928e000001957db5d89fc6189569&docguid=I927c3e80e10a11eaad20d1cf72cae2ef&hitguid=I927c3e80e10a11eaad20d1cf72cae2ef&spos=1&epos=1&td=1&context=11&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1

2. Andrea, G. F. M., Arquite, H. R. L., & Camargo, J. M. (2020). Proteção dos dados pessoais como direito fundamental: A evolução da tecnologia da informação e a Lei Geral de Proteção de Dados no Brasil. Revista de Direito Constitucional e Internacional, 121, 115-139. rdci-121-gianfranco-andrea-e-outros.pdf

3. Brasil. (2018). Lei n.º 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Diário Oficial da União. https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm

4. Búrigo, A. B., & Carloto, S. (2023). A efetividade dos direitos fundamentais e a proteção à privacidade no contexto das relações de trabalho: Uma análise à luz da Lei Geral de Proteção de Dados Pessoais (LGPD). Revista dos Tribunais, 1057, 137-149. https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89817e000001957db7c6ed2dd30297&docguid=I03dba9f0793111ee918cf16d96029b87&hitguid=I03dba9f0793111ee918cf16d96029b87&spos=1&epos=1&td=1&context=21&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1

5. Calabrich, B. F. C. (2020). Discriminação algorítmica e transparência na Lei Geral de Proteção de Dados Pessoais. Revista de Direito e as Novas Tecnologias, 8, 1-20. https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89817e000001957db819514bddd0a3&docguid=I01c65d10d2a711eaa3bfd5d545d9a492&hitguid=I01c65d10d2a711eaa3bfd5d545d9a492&spos=1&epos=1&td=1&context=31&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1

6. Cardoso, O. V. (2022). Responsabilidade civil na Lei Geral de Proteção de Dados Pessoais. Revista de Direito Privado, 111, 109-123. http://revistadostribunais.com.br/maf/app/document?stid=st-rql&marg=DTR-2022-5147

7. Cardoso, O. V. (2023). O ônus da prova na Lei Geral de Proteção de Dados Pessoais. Revista dos Tribunais, 1047, 161-175. https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89b1d5000001957dc7a6804554ff6b&docguid=I4842fee0770711ed8f58bed88a734e4b&hitguid=I4842fee0770711ed8f58bed88a734e4b&spos=1&epos=1&td=1&context=199&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1

8. Cavet, C. A., & Faleiros Jr., J. L. M. (2024). A publicidade direcionada por dados à luz da Lei Geral de Proteção de Dados Pessoais. Revista de Direito do Consumidor, 154, 161-187. https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89817e000001957db953026e651e6e&docguid=I587f0da05e9e11ef9715ee068a6b1ec0&hitguid=I587f0da05e9e11ef9715ee068a6b1ec0&spos=1&epos=1&td=450&context=50&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1

9. Cerqueira, J. S. (2022). A confluência entre a Lei de Acesso à Informação e a Lei Geral de Proteção de Dados. Revista de Direito e as Novas Tecnologias, 17, 1-20. https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a898b7e000001957dba2893731103b0&docguid=I5aad61606bb811ed8aac921ee1e5e871&hitguid=I5aad61606bb811ed8aac921ee1e5e871&spos=1&epos=1&td=288&context=66&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1

10. Deienno, R., & Santos, S. Q. dos. (2014). Normas gerais, destinatários, e princípios do acesso à informação. In H. de Almeida, L. de S. Lehfeld, & M. B. Guedes (Eds.), Comentários à Lei de Acesso à Informação (pp. unknown). Santa Cruz do Sul, Brazil: Essere Nel Mondo.

11. Hentges, S., & Coimbra, R. (2022). As novas formas de controle do empregado e a Lei Geral de Proteção de Dados. Revista dos Tribunais, 1041, 241-258. https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a898b7e000001957dbb1ad62f9ba5c8&docguid=I269d8c60e2b511ec8b52abff02381d09&hitguid=I269d8c60e2b511ec8b52abff02381d09&spos=1&epos=1&td=4000&context=84&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1

12. Leal Júnior, J. C., & Penha, R. M. S. (2022). Eficiência, consensualismo e os meios autocompositivos de solução de conflitos na administração pública. Revista dos Tribunais, 1038, 51-67. https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89ca140000019545026d8cd6cdebc7&docguid=Ia9a70620b62a11ec9c2abe4b74fa6f44&hitguid=Ia9a70620b62a11ec9c2abe4b74fa6f44&spos=1&epos=1&td=6&context=53&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1

13. Lucca, N. de, & Martins, G. M. (2024). A proteção dos dados pessoais sensíveis na Lei Geral de Proteção de Dados. Revista de Direito do Consumidor, 153, 15-30.

http://revistadostribunais.com.br/maf/app/document?stid=st-rql&marg=DTR-2024-9337

14. Martins, G. M., & Longhi, J. V. R. (2022). Responsabilidade civil na Lei Geral de Proteção de Dados, consumo e a intensificação da proteção da pessoa humana na internet. Revista de Direito do Consumidor, 139, 101-124. https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a898b7e000001957dbc9b42a3ab7d42&docguid=I7ea41e20628511ecb033c78e1088bbbf&hitguid=I7ea41e20628511ecb033c78e1088bbbf&spos=1&epos=1&td=3&context=109&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1

15. Neves, R. S. (2018). Audiências de conciliação e a fazenda pública: O dogma da indisponibilidade do interesse público do juízo. Revista dos Tribunais, 990, 289-306. https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89ca14000001954505d37f6e1a346a&docguid=I541a77902bf611e8916f010000000000&hitguid=I541a77902bf611e8916f010000000000&spos=1&epos=1&td=1&context=149&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1

16. Oliveira, R. A. de. (2018). Lei Geral de Proteção de Dados Pessoais e seus impactos no ordenamento jurídico. Revista dos Tribunais, 998, 241-261. https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89a3e2000001957dbd4cf3f839a281&docguid=I19df6040ecb711e8810c010000000000&hitguid=I19df6040ecb711e8810c010000000000&spos=1&epos=1&td=1&context=124&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1

17. Ribeiro, R. K. P. V. L. (2022). Responsabilidade civil objetiva dos provedores de aplicação por conteúdo postado por terceiros à luz e sob a vigência do Marco Civil da Internet e da Lei Geral de Proteção de Dados. Revista de Direito e as Novas Tecnologias, 14, 1-20. https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89a578000001957dbdf9a39934ae3e&docguid=I03322750a42011ecbdd68452654b6c9c&hitguid=I03322750a42011ecbdd68452654b6c9c&spos=1&epos=1&td=1&context=140&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1

18. Siqueira Júnior, P. H. (2011). Pós positivismo. Revista do Instituto dos Advogados de São Paulo, 28, 239-265. https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89d21f000001946556f38c616c9db9&docguid=Ibab718e02d2f11e1860900008517971a&hitguid=Ibab718e02d2f11e1860900008517971a&spos=16&epos=16&td=20&context=40&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1

19. Stürmer, G., & Miranda, D. A. P. (2023). A utilização de algoritmos na fase pré-contratual laboral: Uma análise da seleção automatizada de empregados no Brasil e a Lei Geral de Proteção de Dados Pessoais. Revista de Direito do Trabalho e Seguridade Social, 232, 55-68. https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89b480000001957dbf46e9d213573d&docguid=I73e0212077ad11eeb70fca6bfa4e4a9f&hitguid=I73e0212077ad11eeb70fca6bfa4e4a9f&spos=1&epos=1&td=1&context=160&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1

20. Suzin, J. B., & Aguiar, D. M. de. (2023). Dados sensíveis e a telemedicina: Proximações com a Lei Geral de Proteção de Dados. Revista de Direito e Medicina, 14, 1-20. https://www.revistadostribunais.com.br/maf/app/resultList/document?&src=rl&srguid=i0a89a578000001957dc287ec82711080&docguid=I9f0c1490cd2011edae20a0ef97223717&hitguid=I9f0c1490cd2011edae20a0ef97223717&spos=1&epos=1&td=1&context=185&crumb-action=append&crumb-label=Documento&isDocFG=false&isFromMultiSumm=&startChunk=1&endChunk=1

21. Verbicaro, D., & Calandrini, J. (2022). A proteção da confiança do consumidor e a base do legítimo interesse na Lei 13.709/2018 (Lei Geral de Proteção de Dados Pessoais). Revista de Direito do Consumidor, 139, 73-99. https://www.researchgate.net/publication/358748033_A_PROTECAO_DA_CONFIANCA_DO_CONSUMIDOR_E_A_BASE_DO_LEGITIMO_INTERESSE_NA_LEI_137092018_LEI_GERAL_DE_PROTECAO_DE_DADOS_PESSOAIS