Revista da Faculdade de DIREITO da Universidade Federal de Uberlândia

The protection of consumer's personal data and the electronic geodiscrimination practice: geopricing and geoblocking

A proteção dos dados pessoais do consumidor e a prática de geodiscriminação eletrônica: geopricing e geoblocking

Bárbara Guerra Chala[1]
Cíntia Burille[2]
Lucas Moreschi Paulo[3]

Abstract: The purpose of this study is to analyse the General Data Protection Law for the Protection of Personal Data from the perspective of the protection of the consumer's personal data, with a view to ascertaining the main aspects of the legislation and verifying its impacts in relation to geopricing practices and geoblocking. To that effect, it begins by addressing the principles of the new legislation that inform the activity of processing personal data. Right after, the main axes of structuring the law are presented, focusing on aspects that concern the processing of consumer data. Finally, the practices of geodiscrimination will be examined, with the effect of assessing the legal treatment in relation to such techniques and how they may be affected after the entry into force of the General Data Protection Law. For that, the hypothetico-deductive methodology and the bibliographic research technique were adopted. Thus, it is observed that new data protection legislation added to the protection of consumers' rights in relation to the practices of geopricing and geoblocking, insofar as the standard was designed to prevent the disinformation of the personal data holder on the purpose of the treatment of your information and the illegitimate treatment of personal data, as well as covering the possibility of redressing the consumer who holds personal data if he experiences damage.

Keywords: Consumer; Discrimination; Geopricing; Geoblocking; General Data Protection Law.

---

[1] She holds a Master's Degree in Law from Fundação Escola Superior do Ministério Público (FMP), a Post-graduation certificate in Family and Inheritance Law, and Bachelor's Degree in Law by Pontifícia Universidade Católica do Rio Grande do Sul (PUCRS). She currently works as a clerck at the Rio Grande do Sul's State Court (TJRS).

[2] She is a Master's Degree in Laws candidate at Fundação Escola Superior do Ministério Público (FMP). She holds a Post-graduation certificate in Family and Inheritance Law by Fundação Escola Superior do Ministério Público (FMP), a Post-graduated in Civil Law and Civil Procedure, and a Bachelo Degree in Laws from Centro Universitário Ritter dos Reis (UniRitter). Lawyer.

[3] He is a Master's Degree in Laws candidate at Fundação Escola Superior do Ministério Público (FMP), with a scholarship. He holds a Bachelor Degree in Laws from Fundação Escola Superior do Ministério Público (FMP). He currently holds a research scholarship at the Research Group Fundamental Rights Collision and Law as Argumentation, coord. by Prof. Dr. Anizio Pires Gavião Filho. Lawyer.

DOI: http://dx.doi.org/10.14393/RFADIR-v49n1a2021-62777

Resumo: O presente estudo tem por escopo analisar a Lei Geral de Proteção de Dados Pessoais sob o prisma da tutela dos dados pessoais do consumidor, com o fito de averiguar os principais aspectos da legislação e verificar os impactos desta em relação às práticas de geodiscriminação eletrônica. A esse efeito, inicia-se abordando os princípios da novel legislação que informam a atividade de tratamento de dados pessoais. Logo após, são apresentados os eixos primordiais de estruturação da lei, com foco nos aspectos que dizem respeito ao tratamento de dados pessoais dos consumidores. Por derradeiro, adentra-se no exame das práticas de geodiscriminação, ao efeito de aferir qual o tratamento jurídico destinado a tais técnicas e como elas poderão ser afetadas a partir da entrada plena em vigor da Lei Geral de Proteção de Dados Pessoais. Para tanto, adotou-se a metodologia hipotético-dedutiva e a técnica de pesquisa bibliográfica. Desse modo, observa-se que a nova legislação agregou à tutela dos direitos dos consumidores em relação às práticas de *geopricing* e *geoblocking*, na medida em que a norma foi arquitetada no sentido de impossibilitar a desinformação do titular de dados pessoais sobre a finalidade do tratamento das suas informações e o tratamento ilegítimo dos dados pessoais, bem como abarcou a possibilidade de reparação do consumidor titular de dados pessoais nas hipóteses em que venha a experimentar danos.
Palavras-chave: Consumidor; Discriminação; *Geopricing*; *Geoblocking*; Lei Geral de Proteção de Dados Pessoais.

1. Introduction

Since we are born it is registered and saved lots of personal data in public and private subscriptions, that goes from our name up until data about our medical records, school records, taxations, labours, political views, criminal records, amongst others. Decades ago, much of this information was stored only in physical records on paper, a circumstance that, gradually, after the computer's releasing and the advancement of technological and communication means, has been replaced by electronic records, so that access and sharing of personal data expanded abruptly and very significantly.

Technological and informational development, as well as globalization, undeniably brought many facilities to the daily lives of individuals and made possible the storage of a large volume of information and the data flow, which can be disseminated instantly and on a large scale,

crossing barriers. In addition, the technological expansion and maturation generated a socioeconomic advance of information and caused important reflexes in consumer relations, with personal data assuming the essential input figure of the current digital economy that has taken over society.

In this context, in which personal data assumed a strategic importance to move economic activities, allowing production efficiency and creating new forms of intersubjective and commercial relationships, the law is faced with new challenges. Among them, the need to provide adequate protection of the personal data of individuals and to effectively protect the consumer in the face of innovative practices of suppliers in the scope of electronic commerce.

Therefore, the General Data Protection Law (LGPD[4]) in Brazil is formulated, following the European model, with the purpose of changing the paradigm of indiscriminate treatment of personal data, preventing the occurrence of damage, and safeguarding the rights of individuals. On the other hand, the abusive practices of suppliers are improved, based on the use of personal data, including the geodiscrimination techniques.

Thus, the analysis of the LGPD and the examination of its interlocution with the recent practices of geopricing and geoblocking are essential, which, although they have the potential to significantly affect consumers, have not yet been the subject of extensive studies in the country. The objective is, therefore, to verify how the new legislation impacts and can add to the protection of the consumer in prohibition of geodiscriminatory techniques.

To this end, in the present study, a broad approach to LGPD will be carried out, starting with the explanation of the principles that have come to guide the activity of personal data processing in Brazil. Then, the main axes that structure the activity of personal data processing will be exposed, based

[4] Lei Geral de Proteção de Dados in portuguese.

on the regulation conferred by the new legislation, with a focus on aspects that concern the protection of the consumer who holds personal data.

Soon after, the practices of geopricing and geoblocking will be presented and the legal treatment for such techniques applied by suppliers in the context of the digital economy will be investigated. In the end, the objective is to verify if the LGPD collaborates in the protection of the data holder consumer in the face of geodiscrimination practices. For this, the hypothetico-deductive methodology and the bibliographic research technique were adopted.

2. Principles that inform the personal data processing

The General Data Protection Law (LGPD) appears in the legal system to regulate the treatment of personal data in Brazil, covering, alongside the Consumer Protection Code, the Habeas Data Law, the Positive Registration Law, the Access to Information and the Internet's Civil Milestone Regulation, the microsystem of protection of personal data in the Country. Inspired by the European model, consistent with the General Data Protection Regulation, the new legislation proposes general rules of national interest and aims to protect the fundamental rights of freedom and privacy, as well as the free development of the natural person.

The law defines milestones for the use of personal data, with a focus on guaranteeing the personality rights of individuals, notably the right to privacy in its double meaning (right to be left alone and informational self-determination), without implying that the. communicative rights are curtailed, as well as offering bases for the adequate economic and technological development, from the establishment of "a normative dialectic of conciliation between all these elements" (BIONI, 2019, p. 110). The purpose of the legislation, therefore, is to "provide guarantees for citizens' rights, while providing the basis for the development of the information

economy, based on the vectors of trust, security and value" (MENDES; DONEDA, 2018, p. 470).

Adopting an expansionary and dynamic concept of personal data, the Brazilian standard protects data referring to natural persons, identified or identifiable, processed by public or private databases. Thus, it covers not only the personal data that are associated with the natural person - through direct identifiers that differ an individual -, but also those that potentially lead to the individualization of the person - considering the use of reasonable and available technical means at the time of treatment – with the exclusion of anonymized data.

With the purpose of regulating the activity of processing personal data and taking into account that the digital environment undergoes continuous changes and updates, a circumstance that hinders the broad legislative follow-up, LGPD salutary established guiding principles to this activity, with the objective of wrapping up innovations and technological advances and satisfying individuals.

It can be said that there is an international convergence in relation to the basic principles tangent to data protection that should guide the processing activity, limiting it and giving the individual control over the flow of their data (MENDES; BIONI, 2019, p 06). The principiological framework, known as Fair Information Practice Principles, had its positivity in the first law to provide on data protection in the world, the Hesse State Law, in Germany, in the nineteen-seventies, and since then they have been provided for in legislation similar principles to guide the treatment of such data (MENDES; BIONI, 2019, p. 08).

In this context, the protective Brazilian law provides data eleven principles that should inform all personal data processing activity (art. 6/LGPD), from collection to disposal. Among them, it repeats the principles present in the European regulation and establishes three different ones: the

principle of security, the principle of prevention and the principle of non-discrimination (MENDES; BIONI, 2019, p. 08).

Going into the specific analysis of the principles foreseen in the legislation that serve as a guideline of operability in the treatment of personal data and provide the survival of the law over time, it is stated that the activities of processing of personal data must, initially, observe the good faith. In this case, the principle of good faith is based on the protection of the legitimate expectations of the personal data holder vis-à-vis the controller, which is outlined based on the concrete circumstances in which consent was given, the purpose of using and processing the data that was indicated at the time, as well as how the previous information offered was understood (MIRAGEM, 2019, p. 177), considering its possible vulnerability.

In addition, said activities must comply with the principle of purposiveness, according to which the processing of personal data can only be carried out with a legitimate, certain, and previously informed purpose to the data holder. In this way, the person who intends to obtain the consent of the data holder is obliged to inform him expressly about the purpose for which he intends to use the information, binding on the terms of his manifestation.

The processing of personal data also needs to be compatible with the finalities informed to the data holder when consenting to the use of the data or prior to processing in other legal cases, satisfying the principle of adequacy. This is because the adequacy is linked to the "situation of trust that is created by strict compliance with the terms of the information prior to consent or informed use" (MIRAGEM, 2019, p. 181).

The principle of necessity, in turn, embraces the idea of minimal intervention in the individual sphere, signalling that the personal data processing must be restricted to the minimum necessary to meet the proposed purposes. In addition to these rules, the principle of transparency advocates the necessary transparency about the data processing procedure

and the individual involved in the activity, linking to it the principle of free access, which translates into the right to free and easy consultation of the holder on the completeness of his personal data, as well as on the form and duration of their treatment.

In the same sense, the principle of data quality demands the indispensability of accuracy, clarity, relevance and updating of any individual's personal data, a circumstance that is especially important when considering the permanent and continuous nature of the data processing and the natural modification of these data. in everyday life, bringing the burden of maintaining its quality to the controller (MIRAGEM, 2019, p. 183). Throughout the new law, the rule translates into the right of the holder to correct his personal data that was collected by the treatment agents.

The principle of security in compliance with the preventive character of the standard, is linked to the need for zeal for the security of personal data, requiring the adoption of security and protection measures in the treatment of this information. In the scope of consumer relations, this principle is associated with the general duty of quality of the supplier's service provision, unfolding in the duty of security in relation to his person and assets (MIRAGEM, 2019, p. 184). In the same vein, the principle of prevention relates to the need to prevent damage from occurring during the processing of personal data.

Regarding to the principle of non-discrimination, it demonstrates the impossibility of processing personal data for discriminatory, illegal, or abusive purposes. In consumer relations, therefore, the advantage of the supplier with the processing of personal data, with the significant increase in the accuracy of segmentation and personalization of consumers, cannot serve to harm, restrict, or exclude any consumer from the possibility of access to consumption (MIRAGEM, 2019, p. 185).

Last but not least, the principle of accountability and accountability requires treatment agents to demonstrate compliance with and compliance with the rules on the protection of personal data, as well as the effectiveness of the measures adopted. Among the abovementioned protective norms, it is important to emphasize for the purposes of this study the protection of the consumer, expressly provided for among the fundamentals of the LGPD.

3. Main axis of the general data protection regulation (LGPD)

Having examined the principles that inform the processing of personal data and constitute, together with the rights of the data holder, one of the axis around which the protection of personal data established by the LGPD is structured, it is necessary to enter into the analysis of the other pillars that articulate the protection of personal data, in order to provide an overview of the regulation of the subject, they are: 1) unity and generality of the application of the law; 2) legitimation for data processing; 3) rights of the holder; 4) obligations of personal data processing agents; and 5) responsibilization of personal data processing agents (MENDES; DONEDA, 2018, p. 470-471).

The LGPD can be defined and characterized by its generality and unit. This is because "the law focuses on the protection of citizens' data, regardless of who carries out its treatment, thus applying to both the private and public sectors, regardless of the data treatment modality" (MENDES; DONEDA, 2018, p. 471).

The indistinct and horizontal application of the law - with some express exceptions foreseen in it and which are shaped in a way that does not compromise its integrity - guarantees, on the one hand, the security of natural persons holding personal data and, on the other hand, provides isonomy among the entities - public and private - that carry out the

processing of personal data (MENDES; DONEDA, 2018, p. 471), circumstances that prove to be largely beneficial to all.

Adopting the ex-ante protection model (MENDES; BIONI, 2019, p. 166), Brazilian law established authoritative hypotheses for the processing of personal data, without which treatment agents cannot perform it. Ten normative bases authorizing the processing of personal data in Brazil were provided for that, they are: a) with the consent of the holder provided in writing or by another means that demonstrates the manifestation of will of the holder; b) due to compliance with legal or regulatory obligation by the controller; c) for the execution of public policies; d) to carry out studies by research bodies; e) for the performance of the contract to which the holder of the personal data is a party; f) regular exercise of rights in judicial, administrative or arbitration proceedings; g) protection of life or physical safety; h) for health protection; i) legitimate interest; and j) credit protection.

In comparison with European law, the hypotheses that legitimize the processing of personal data in Brazil are highly similar, with the difference that the national law has four additional legal bases, namely: the conduct of studies by a research body, the exercise regulating rights in process, health protection, and credit protection (MENDES; BIONI, 2019, p. 165). It is important to the present study, however, to examine only the five hypotheses that are most related to consumer law, from which the cases in which the consumer as an information holder will be protected by LGPD are verified.

In fact, the processing of personal data is primarily permitted in cases where the holder of the information agrees with the activity, through free, informed, unequivocal and for a determined purpose, manifestation. The imperfect formation of this volitional element is considered a flaw in the consent and makes it null (TEFFÉ; VIOLA, 2020, p. 10).

By means of the free consent, it appears that the consent action must be spontaneous, free from any pressure and characterized by free will in the choice of the personal data holder (BIONI, 2019, p. 197), who has the choice between accepting and refuse the use of your property (TEFFÉ; VIOLA, 2020, p. 7). The statement of the holder, moreover, needs to be informed, preceded by transparent communication about the treatment of personal data, since "information is a determining factor for the expression of a free and conscious consent, directed to specific treatment, for a specific agent and under certain conditions" (TEFFÉ; VIOLA, 2020, p. 9).

In addition to these volitional characteristics, it is essential that the manifestation of agreement with the processing of personal data is perceptible by the holder, that is, unequivocal, understood by him as such (MIRAGEM, 2019, p. 191) and without ambiguity (TEFFÉ; VIOLA, 2020, p. 10). Thus, in consumer relations through digital means, it is required that the form or moment of the consent to be properly identified (MIRAGEM, 2019, p. 191).

The data protection legislation also requires that the declaration of the data holder's will have a direction, being treated for a determined purpose, since the individual cannot consent in a vacuum and in a generic way (BIONI, 2019, p. 198). Qualified the voluntary manifestation of the personal data holder with all the mentioned requirements, by writing or in a detached clause of the other contractual provisions, or by another means that demonstrates its agreement and consent.

In some cases, nonetheless, considering the high risk of processing personal data, a "special consent - even more explicit -" (BIONI, 2019, p. 239) and specific is required, due to the peculiar nature of the data being processed (sensitive data) or due to the vulnerability of the data subject (data from children and teenagers).

With regard to sensitive data, the special discipline intended by the General Law for the Protection of Personal Data, regarding consent and in

relation to other peculiarities, "aims to prevent and reduce the risks of discrimination due to the criteria prohibited by the Constitution, from the strictest delimitation of the conditions of its treatment" (MIRAGEM, 2019, p. 196). This is because the circulation of sensitive personal data causes a greater risk to the individual's personality, especially if they are used with discriminatory intent.

For the treatment of child and teenager data at the time of consent, it must be verified by at least one of its parents or by their legal representative. However, if the minor's data is treated precisely to contact his parents or guardians feasible, or even for his protection, the possibility of collecting it without consent is allowed, provided that such data are not passed on to third parties, stored, and used only once.

More than that, there is also a general situation in which the consent of the personal data holder is relinquished, which occurs when the individual makes it manifestly public. Even in this atypical hypothesis, the rights and guiding principles of the new legislation must be safeguarded and respected.

Structural hypothesis of legitimation for the processing of personal data, the manifestation of consent of the personal data holder is very present in consumer relations, which is why it has gained outstanding attention in the present study. However, it is not just consent that makes the processing of the consumer's personal data possible.

Data processing is also allowed when it proves necessary for the performance of a contract to which the personal data holder is a party, or in preliminary contractual procedures. Another important situation that legitimizes the processing of personal data arises when the activity is necessary to serve the legitimate interests of the controller or of a third party, except in the event of the fundamental rights and freedoms of the holder prevailing that require the protection of information. The legitimate interest hypothesis gained in legislation "the status of a new" regulatory

wild card "to embrace a myriad of possible uses of the data" (BIONI, 2019, p. 249).

Despite these assumptions, the processing of consumers' personal data proves to be equally viable for the regular exercise of these rights in judicial, administrative and arbitration proceedings, as well as for credit protection, which is the most traditional purpose in Brazil and was already in a way regulated through the Consumer Protection Code and the Positive Registration Law.

Authorized the processing of data, due to one of the ten mentioned legitimizing hypotheses foreseen in the LGPD, the rights of the holder of such information during its use must be safeguarded. In Brazil, several rights are provided for the benefit of the personal data holders, which are remarkably similar to those provided for in the European regulation.

The holder has, principally, the right to confirm the existence of treatment of his personal data. Obtaining information about the processing of the data will occur upon the express request of the owner, or his legal representative, to the processing agent, who may postulate a simplified statement, to be answered immediately, or a complete statement that ordinarily must be answered in fifteen days in electronic or printed form.

In addition to confirmation, the personal data holder also has the right of access to data about him/her that the controller has, as well as the way in which it will be processed, through free and easy consultation. As with confirming the existence of data processing, the data subject may require a simplified or complete statement.

With access to your data, if the holder observes the incorrectness of the information, due to incompleteness, inaccuracy or outdated, he has the right to demand the rectification of the data, by means of an application. And, if the treatment agent who received the application previously shared the incorrect data, he has the duty to immediately communicate to everyone with whom he has shared so that they adopt the same correction procedure.

In parallel, the personal data holder also has the right to postulate the portability of his information. The portability of personal data occurs, above all, in the scope of consumer relations, from one product or service supplier to another, at the request of the consumer, who now has the power to conclude a new contract taking with him the relevant information from the previous adjustment, ensuring their freedom of choice in the market, and enabling the provision of services according to their needs (MIRAGEM, 2019, p. 23).

The elimination of personal data at the end of their treatment is also right holder, as well as the elimination of personal information unnecessary, excessive, or treated not in accordance with the law, and these last three hypothesis the holder also has the possibility to postulate the anonymization or blocking of such data. The conservation of data is authorized, however, especially in consumer relations, for the exclusive use of the controller, being forbidden to access it by a third party, and provided that the data is anonymized.

Regarding the rights to obtain information, the personal data holder has the right to request clarification on the sharing of his data with public or private entities, as well as on the possibility of not consenting to the processing of data and, therefore, about the consequences of your denial. Even in cases where the data subject regularly agrees with the processing activity, through free, informed, unequivocal and for a determined purpose, at any time he has the right to revoke the informed consent. This is because the right to revoke consent is inherent in the informational self-determination of the personal data holder and must be made possible by a free and facilitated procedure.

The LGPD does not cover, however, only rights to the holders of personal data, but also obligations to the agents that carry out the activity of processing the information. The obligations imposed on treatment agents are intended to regulate the efficient functioning of the activity, mainly with

the aim of preventing the occurrence of damage to the holders of personal data, and it is important to mention in this study some essential ones.

In fact, treatment agents must adopt appropriate security measures to protect personal data from unauthorized access and from accidental or unlawful situations of destruction, loss, alteration, communication, or any form of inappropriate or illicit treatment. In addition, the controller has the obligation to report to the National Data Protection Authority (ANPD[5]) in the event of a security incident that may cause significant risk or damage to the holders of personal information, such as, for example, in the event of data leak. Thus, the Authority, after verifying the severity of the incident, may determine the adoption of measures to reverse or mitigate the effects of the incident or, also, the wide dissemination of what happened in the media. The law also requires the controller to carry out a privacy impact report, when requested by the National Data Protection Authority, which must include, at a minimum, a description of the type of data collected, the methodology used for capturing and guaranteeing security, listing the measures adopted for security and mitigation.

It is evident, throughout the normative text of the LGPD, its preventive character and its constant concern and encouragement in preventing risks, mitigating damages, and spreading a culture of good practices. In this context, a system called active responsibilization has been developed, as not breaking the law is no longer sufficient, and it is essential to demonstrate the proactive prevention of the occurrence of damage (BODIN DE MORAES, 2020).

However, it seems inevitable that, in some cases, despite the precautions taken by treatment agents to prevent and prevent damage from occurring, personal data holder will experience damage because of the data processing activities. Thus, to protect them in these cases, the LGPD brings

[5] Autoridade Nacional de Proteção de Dados in portuguese.

an objective liability regime, in which there is no investigation of the guilt of the treatment agents.

The operator, as an agent that carries out the processing of personal data, will only be liable to us for acts that commit that are contrary to the law or to the instructions provided by the controller, in which cases there is joint liability between controller and operator. The controller, as an agent that emanates the treatment order, is responsible for the other hypotheses and, in the event of more than one controller, both respond jointly (MENDES; DONEDA, 2018, p. 474).

The liability of the processing agents will only be removed when one of the exclusions provided for in the law applies, that is, when the agents prove that they did not perform the processing of personal data, or demonstrate that, even though they performed the treatment, there was no violation of the data protection legislation, or that the damage is due to the sole fault of the data subject or third party.

4. The digital geodiscrimination practices

Undeniable that, over the past few years, internet users increasingly become consumers, proof of this fact is the exponential increase in electronic commerce, which generates in the consumer the feeling of freedom and a comprehensive power of choice. In Brazil, it is observed that only between the years 2012 and 2018 “there was a growth of about 19 million Internet users who performed this activity” (COMITÊ GESTOR DA INTERNET NO BRASIL, 2018, p. 103).

The increase in electronic commerce, combined with new practices for processing personal data of individuals and the innovative technologies available, has launched crucial challenges in the scope of consumer law. This is because suppliers, in the digital context of the information society, began to collect and process more and more consumer data, as well as to use

new, sometimes aggressive, and forged techniques, to profile and segment them, according to their purchase pattern, their location, the interaction they make on social networks and various other data available on the world wide web.

The collection and processing of data from e-commerce companies, on the one hand, adjusts the market research tailored to the wishes of each consumer, in order to personalize their experience on the internet, a circumstance that most of the time gives them it is beneficial (FORTES; MARTINS; OLIVEIRA, 2019, p. 237), as it brings convenience. However, despite the disguise constituted by freedom of choice and the offer of prices as a result of the competitiveness between the different market players, the virtual ecosystem in which electronic commerce occurs also enables the elaboration of consumer profiles and enables the manipulation of offers by large companies (FORTES; MARTINS; OLIVEIRA, 2019, p. 238), in benefit of their activities, based on the personal data processing.

In this economic perspective, it is stated that "the possession of personal data acquires increasing value" (MIRAGEM, 2019, p. 175) and these can be considered as the new oil of the current times, since they are seen as the essential substance for most economic activities currently practiced (FRAZÃO, 2019, p. 24), causing a strong influence on consumer rights. "Information is power, an instrument of control and currency of exchange in the 21st century" (MARTINI; BERGSTEIN, 2019, p. 167), which has a totally "informational, global and networked" economy (CASTELLS, 2002, p. 119).

A curious illustration that makes the visualization of personal data accessible as the new commodity of the current times is the calculator developed by the Financial Times newspaper[6], in 2015 and updated in 2017, "with the objective of stipulating, in a critical way, the value of personal

[6] The calculator tool is still available: <https://ig.ft.com/how-much-is-your-personal-data-worth/>. Accessed in: May, the 11th, 2020.

data, taking into account the individual's personal information, in a scenario of true monetization of personality" (REGIS, 2020, p. 68).

Among the commercial practices that have developed in the context of the information society and are commonly applied by suppliers based on personal data captured from consumers, this study has chosen to focus on those that consist of digital geodiscrimination. The choice is due to the fact that such practices were only made possible through the processing of consumer's personal data, specifically its geographical position when purchasing products or services on sites on the Internet (DIAS; NOGUEIRA; QUIRINO, 2019, p. 74).

The geopricing consists in determining prices for different range of products and services, e-commerce, without just cause, based on user location. The geoblocking, in turn, "can be defined as the commercial practices set that prevent certain consumers to access and/or purchase goods or services through an interface online, based on the customer's location" (FORTES; MARTINS; OLIVEIRA, 2019, p. 239).

With the internet's omnipresence, which has now been accessed from the most diverse electronic devices, in addition to the possibility of monitoring the geographic location of these devices, the practices of geopricing and geoblocking began to be verified everywhere across the globe. One of the first cases that get great attention for the abusive and discriminatory practice of charging different prices to consumers, for the same products, based on geographic criteria, occurred in 2000, and was perpetrated by the famous company Amazon, which, after the discovery, returned the money to consumers and apologized to them, publicly committing to never use geographic data to build their pricing policy (FORTES; MARTINS; OLIVEIRA, 2019, p. 238).

In Brazil, the most emblematic case on the subject and which was widely publicized by the media (PAMPLONA, 2018), occurred in 2018, when the Public Prosecutor's Office filed a public civil action against the e-

commerce company Decolar.com, alleging an offense to the diffuse interests of consumers. The *parquet* justified its legal claim in the active geodiscrimination of consumers that was being perpetrated by the business society in the electronic ticket sales and hotel reservation service, through the practices of geoblocking and geopricing, in the extent that these practices were used to manipulated offers, with the usage of technologies information and communication, not offering, or by offering higher price tickets and lodgings for some consumers of certain localities compared to others who just lived in a different location.

In this case, consumers would not have been informed about the gathering of their personal data and about the fact that information related to their geographic location would be used for supplier pricing, nor for blocking offers, as is commonly done in geodiscrimination practices. In this light, the Public Prosecutor's Office postulated the express declaration of illegality of the practices and the payment of compensation to the injured consumers, and, until the conclusion of this study, the class action is still in progress and was the only one that has already led to the judgment of the Superior Court of Justice such techniques, which are very recent, although the decision is outlined to the present discussion. At the same time, the company Decolar.com was ordered by the Department of Consumer Protection and Defence to pay a million-dollar fine, in the amount of seven million and five hundred thousand reais (DIAS; NOGUEIRA; QUIRINO, 2019, p. 74), due to the use of these digital geodiscrimination practices.

In this panorama, it is possible to affirm that, before the promulgation of the LGPD, the prohibition of the practices of electronic geographical discrimination of consumers was initially supported by the Federal Constitution, through the constitutional principle of equality and the right to equality, protected in article 5. In addition, Article 170 of the Constitution also repudiates any discriminatory practice, to the extent that

it provides that the economic order must seek to reduce regional and social inequalities, as well as advocating consumer protection.

In the infra-constitutional scope, the Consumer Protection Code also goes against those practices since it preserves non-discrimination and the right to information as basic consumer rights. More than that, the Diploma prohibits the supplier's abusive practices of refusing to fulfil consumer demands and of rising the price of products or services without a good reason.

In the same sense, consumer protection norms against geodiscriminatory practices were found in the Internet's Civil Milestone Regulation, which guarantees as user rights, among others, the information and protection of their personal data, which can only be used for purposes that: a) justify its gathering; b) are not prohibited by law; and c) are specified in the service provision contracts or in terms of use of the internet applications. The law also guarantees the isonomic treatment of the transmission, switching or routing of any data packets, without distinction by content, origin and destination, service, terminal, or application.

In addition to the consumer protection spectrum, the geopricing and geoblocking represent unfair competition, because they cause losses to other companies in the same industry that do not benefit from the illegality. The techniques, therefore, can constitute a crime of unfair competition, in accordance with the provisions of article 195, III, of Law 9.279/1996. Furthermore, according to the rules of Law 12.539/2011, which regulates the Brazilian Competition Protection System, it constitutes an infraction of the economic order, regardless of fault, the acts limit, distort or impair free competition or free enterprise.

With this normative framework, it was already possible to seek consumer protection against the occurrence of geodiscrimination practices, as the *parquet* did when sued the class action against Decolar.com, ensuring that the supplier offers same treatment conditions to all buyers. It is

questioned, however, whether now, with the arrival of the LGPD, there will be a more effective consumer protection.

Although there is no prohibition and express regulation of such techniques in the new legislation, the answer is positive, as the LGPD brings greater support to the consumer, safeguarding it. The legislation initially protects the consumer, insofar as it precludes the impossibility of processing personal data for discriminatory, illegal, or abusive purposes, through the principle of non-discrimination. Still in this area, the principles of transparency and purposiveness ensure that the consumer personal data holder receives clear and accurate information about the treatment of his information and for what purpose it will be used, which must be legitimate, specific, and explicit, rules that direct against how geopricing and geoblocking practices occur.

Furthermore, in order to legitimize the processing of personal data related to the consumer's location, it would be necessary, in compliance with the LGPD, that the holder of the information had given his prior, free, informed, unambiguous and for a determined purpose, which, in the verified situations of geopricing and geoblocking never occurs. Thus, it is observed that the law imposes yet another limitation on the use of information related to the consumer's location. Through the LGPD, it is also possible to repair the consumer with personal data who experiences any damage - moral or material, individual or collective - as a result of discriminatory geolocation practices that have taken advantage of the irregular treatment of personal data.

In this context, it is concluded that the new legislation appears in favour of the rights and guarantees of the consumer data holder, who presents himself as "(hyper)vulnerable in the midst of this information market" (BIONI, 2019, p. 165) and, in the absence of a specific rule forbidding geodiscriminatory practices, you can use the LGPD to protect your interests.

5. Final Remarks

In the current hyperconnected world in which we live, the discussion on the protection of personal data has become fundamental, notably because the information of individuals has become a key part of the current economic configuration. As demonstrated, the Brazilian's personal data has been collected and processed to promote different practices of suppliers in the context of electronic commerce, some of them abusive and spurious, such as geopricing and geoblocking.

The LGPD, thus, was inaugurated in the national legal system to regulate the activity of processing personal data, filling a long-standing legal gap in the country. With the purpose of launching guidelines for the activity, the legislation formulates eleven important principles to govern and keep it active. Divided into five main structuring axes, the new general legislation foresees the authorizing hypotheses for the processing of personal data, encompasses the rights of the data holder and imposes obligations on the processing agents, as well as formulates a liability regime in case of damage to the data subject on the occasion processing of your personal information.

Undeniable, so the immense impact that LGPD brought, bringing many changes and parameters with respect to the processing of personal data with the aim of preventing violations of the rights of individuals and at the same time allow proper and safe economic development and technological. In this line, we sought in the present study to focus on the specific effects of the new legislation in relation to digital geodiscrimination practices, which put the individual's rights at risk, both as a consumer and as a data holder.

It can be concluded that the practices of digital geodiscrimination were already prohibited and despised by Brazilian law. However, this impediment is reinforced with the advent of the LGPD which, in addition to

protecting the interests of consumers with personal data more effectively, enables the adequate and comprehensive repair of these in the event of damage initiated from the treatment of the personal data of the individual.

Society now has an important role, it needs to assimilate the new regulation, that brings legal security not only to citizens, but also to treatment agents, and now it must adapt to this new reality that will certainly protects data holder consumers' interests more adequately and effectively, contributing to the prohibition of discriminatory treatment of digital consumers. Therefore, a legitimate culture of protection of personal data must be developed in Brazil, with technological progress being guided by the ethics of liability and by the ethics of accountability.

References

BIONI, Bruno Ricardo. **Proteção de dados pessoais**: A função e os limites do consentimento. São Paulo: Forense, 2019.

BODIN DE MORAES, Maria Celina. LGPD: um novo regime de responsabilização civil dito "proativo". Editorial à **Civilistica.com**. Rio de Janeiro: a. 8, n. 3, 2019. Disponível em: <http://civilistica.com/lgpd-um-novo-regime/>. Acesso em: 22 abr. 2020.

BRASIL. Superior Tribunal de Justiça. **Recurso em Mandado de Segurança n. 61.306/RJ**. Relator Ministro Luis Felipe Salomão. Brasília, 10/12/2019. Disponível em: <https://scon.stj.jus.br/SCON/decisoes/toc.jsp?livre=GEOPRICING&b=DTXT&thesaurus=JURIDICO&p=true_>. Acesso em: 13 maio 2020.

CASTELLS, Manuel. **A Sociedade em rede.** A era da informação: economia, sociedade e cultura. vol. 1. 6. ed. rev. e atual. Trad. Roneide Venâncio Majer. São Paulo: Paz e Terra, 2002.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Pesquisa sobre o Uso das Tecnologias de Informação e Comunicação nos Domicílios Brasileiros**: TIC Domicílios 2018. São Paulo: Comitê Gestor da Internet, 2018.

DIAS, Daniel; NOGUEIRA, Rafaela; QUIRINO, Carina de Castro. Vedação à discriminação de preços sem justa causa: uma interpretação constitucional e útil do art. 39, X, do CDC. **Revista de Direito do Consumidor**. São Paulo, Revista dos Tribunais, v. 121, p. 51-97, jan./fev. 2019.

FORTES, Pedro Rubim Borges; MARTINS, Guilherme Magalhães; OLIVEIRA, Pedro Farias. O consumidor contemporâneo no show de truman: a geodiscriminação digital como prática ilícita no direito brasileiro. **Revista de Direito do Consumidor**. São Paulo, Revista dos Tribunais, v. 124, p. 235-260, jul../ago. 2019.

FRAZÃO, Ana. Fundamentos da proteção de dados pessoais – Noções introdutórias para a compreensão da importância da lei geral de proteção de dados. In: TEPEDINO, Gustavo; FRAZÃO, Ana; OLIVA, Milena Donato (Coord.). **Lei Geral de proteção de dados pessoais e suas repercussões no direito brasileiro.** São Paulo: Revista dos Tribunais,

2019.

HOW much is your personal data worth? **Financial Times**, Londres, 12 jun. 2015. Disponível em: <https://ig.ft.com/how-much-is-your-personal-data-worth/>. Acesso em: 07 abr. 2020.

MACHADO, Diego; DONEDA, Danilo. Proteção de dados pessoais e criptografia: tecnologias criptográficas entre anonimização e pseudonimização de dados. **Caderno Especial – A Regulação da Criptografia no Direito Brasileiro**. São Paulo, Revista dos Tribunais, v. 1, p. 99-128, dez. 2018.

MACHADO, Fernando Inglez de Souza; RUARO, Regina Linden. Publicidade comportamental, proteção de dados pessoais e o direito do consumidor. **Conpedi Law Review**. Braga, v. 3, n. 2, p. 421-440, jul./dez. 2017.

MARTINI, Sandra Regina; BERGSTEIN, Laís. Aproximações entre o direito ao esquecimento e a Lei Geral de Proteção de Dados Pessoais (LGPD). **Revista Científica Disruptiva**, v. 1, n. 1, jan./jun. 2019.

MENDES, Laura Schertel; BIONI, Bruno R. O Regulamento Europeu de Proteção de Dados Pessoais e a Lei Geral de Proteção de Dados Brasileira: Mapeando Convergências na Direção de um Nível de Equivalência. **Revista de Direito do Consumidor.** São Paulo, Revista dos Tribunais, v. 124, p. 157-180, jul.-ago. 2019.

MENDES, Laura Schertel; DONEDA, Danilo. Reflexões iniciais sobre a nova lei geral de proteção de dados. **Revista de Direito do Consumidor.** São Paulo, Revista dos Tribunais, v. 120, p. 469-483, nov./dez. 2018.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais.** São Paulo, Revista dos Tribunais, v. 1009, p. 173-222, nov. 2019.

PAMPLONA, Nicola. Ministério Público do Rio acusa Decolar.com de manipular preços. **Folha de São Paulo**. Disponível em: <www1.folha.uol.com.br/mercado/2018/02/mp-do-rio-acusa-decolarcom-de-manipular-precos.shtml>. Acesso em: 10 maio 2020.

PEDUZZI, Pedro. Decolar.com é multada em R$ 7,5 milhões. **Agência Brasil**, 18.06.2018. Disponível em: <http://agenciabrasil.ebc.com.br/economia/noticia/2018-06/decolarcom-e-multada-em-r75-milhoes>. Acesso em: 12 maio 2020.

REGIS, Erick da Silva. Linhas gerais sobre a Lei 13.709/2018 (LGPD): objetivos, fundamentos e axiologia da Lei Geral de Proteção de Dados brasileira e a tutela de personalidade/privacidade. **Revista de Direito Privado**. São Paulo, Revista dos Tribunais, v. 103, p. 63-100, jan./fev. 2020.

TEFFÉ, Chiara Spadaccini de; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica.com**. Rio de Janeiro, a. 9, n. 1, 2020. Disponível em: <http://civilistica.com/tratamento-de-dados-pessoais-na-lgpd/>. Acesso em: 13 jul. 2020.

TEIXEIRA, Matheus. Decolar.com é multada por cobrar preços diferentes de acordo com a região. **Jota**. 18 jun. 2018. Disponível em: <https://www.jota.info/jotinhas/decolar-multada-cobrar-precos-de-acordo-com-a-regiao-18062018>. Acesso em: 12 maio 2020.

Artigo recebido em: 11/08/2021.
Aceito para publicação em: 05/09/2021.