Brazil

Felipe Barros Oquendo[1]

Introduction. Personal data protection in Brasil and current challenges.

Like the European Union and several other countries, Brazil has its own legal regulation of personal data, the General Data Protection Law (Portuguese acronym: LGPD). Enacted on August 14, 2018, the law has not yet entered into force. Officially, this was expected to occur on August 15, 2020, according to the current wording of the law. We say "officially" because, with the health and economic crisis caused by the SARS 2 COVID-19 ("new coronavirus") pandemic, and measures of social isolation and restriction of non-essential services, the Brazilian Senate proposed a bill, turned into law in June 10, 2020[2], which, among other topics, determines the extension of the entry into force of the dispositions of the LGPD related to inspection and penalties by the National Data Protection Authority (Portuguese acronym: ANPD) only on August 1, 2021. Also, on April 29, 2020, the Federal Government passed the effective date of the law to May 1, 2021, through the edition of provisional measure N. 959. If the provisional measure is ultimately converted into law, this will be the new date LGPD enters into force.

In any case, it seems inevitable that Brazil, sooner or later, will have a Data Protection Law in place and an ANPD that regulates and supervises compliance with this law. In fact, even if the entry into force of the law is postponed, the Federal Government could take this additional time to make efforts to structure the National Data Protection Authority with prepared personnel, its own budget and so on.

As will be seen in more detail throughout this report, there are numerous points of the LGPD that are perfectly analogous to those of the General Data Protection Regulation 2016/679 (GDPR), in which Brazilian law was clearly inspired, to the point that we can insert without major problems LGPD under the European model and move it away from the California Data Protection Act model or other divergent models.

However, when compared with European countries such as Italy, France, Germany and Scandinavian countries, which counted with laws such as the European Directive of 1995, and, in some cases, even with data protection authorities already existing in the 1990s, Brazil's history with regard to the legal protection of personal data is clearly less developed. This is relevant, because while in the European Union the GDPR emerged as the culmination of coordinated efforts for harmonizing personal data protection by its Member States, evaluating the diversity and the accumulated experience in national jurisdictions that developed spontaneously and independently, in Brazil LGPD appears as an imposition,

[1] The rapporteur would like to thank his colleagues from the Study Committee in Competition from the Brazilian Intellectual Property Association – Anna Carolina Peixoto, Ana Caroline Silva, Cecília Cunha, Juliana Sydow, Letícia Carneiro, Maria Eduarda Junqueira, Marilia Baracat, Raphael Campos, Renata Soraia Luiz e Vanessa Ferro - for the inestimable aid with research and responding the questions.

[2] Federal Law N. 14.010.

however important and welcome, but strange to national issues and debates, as well as to the Brazilian legal culture. This dissonance can cause problems with the implementation of the law and the penalization / inspection of violations.

In Brazil, since at least the 1967 Constitution, the right to privacy and intimacy are considered essential. This provision that has made its way to our current 1988 Constitution (art. 5, especially item X). The Civil Code of 2002 establishes, in articles 11 to 20, several rights called "personality rights", among them the right to one's name, image / voice, and privacy, which are considered non-transferable and cannot be renounced. The holder of an offended personality right may request cessation of the offense and redress for material and moral damages caused by the offender.

Despite the progress represented by the Civil Code of 2002 in relation to the previous one, which established nothing in this sense, there is no specific regulation of private and personal data in this law, such as personal address, purchase and travel history, etc. This, despite the fact that in the 1990s there was already in Italy, whose laws which greatly influenced the text of our Code, a relatively well-developed legislation and authority to protect personal data, not to mention other European countries such as France and Spain.

On the other hand, for a long time a general right to secrecy has been established by sparse laws on bank data, data related to taxes and income, and telephone conversations, requiring a court order for such confidentiality to be exempted. Also worthy of note is the Brazilian Penal Code, which considers the violation of correspondence, the recording and listening of telephone conversations to be a crime, as well as the disclosure of secrecy, including professional secrecy, and the unauthorized invasion of a computer device to obtain, adulterate or destroy information. In fact, with regard to the protection of secrets, it is important to note that business secrets are expressly protected under the Industrial Property Law (LPI), including test data delivered to regulatory bodies linked to the Government.

It is clear from this brief and incomplete enumeration of rules that the obvious and clear violations of privacy and secrecy, as well as the use of data obtained in an improper and unauthorized manner concerning the person and his or her private life, are punishable by law. However, it is also clear that the use of data relating to shopping behavior, travel, telephone number, e-mail address, passwords, electronic documents, medical examination data, among others, is entirely unregulated, with the exception of borderline situations where the bad faith is blatant.

In other words, there was a need to treat the protection of personal data not only punitively, but also to regulate it in more detail, in order to avoid violation of rights and to promote cooperation between those involved, and not only to repress it and compensate for damages caused, a paradigm that generates a huge burden on the data subjects.

Technological advancement and the concentration of digital platforms in the hands of a few transnational players has greatly increased the possibilities of abusive use of personal data and violation of privacy on the internet. This was one of the reasons for the promulgation of the Civil Rights Framework for Internet[3], a Brazilian law which seeks to establish principles, guarantees, rights and duties for the use of the Internet in Brazil.

By the Civil Rights Framework for Internet, the protection of privacy and personal data is expressly provided as a principle that guides the discipline of internet use in Brazil. This principle is detailed in rights conferred by law, such as the inviolability of intimacy and private life, the inviolability and secrecy of the flow of communications over the internet, the right to clear and complete information on the collection, use, storage, treatment and protection of users' personal data, definitive exclusion of personal data that the user has provided to a particular internet application, upon request, at the end of the relationship between the parties, except for the cases of mandatory record keeping provided for by law.

Although it established rights very much in line with the current LGPD, most of these devices depended on subsequent regulation, which was never issued. Nevertheless, proof of the affinity between the Civil Rights Framework for Internet and the protection of personal data is that the bill that eventually turned into the LGPD was initially a reform of the Framework. However, this initial wording of the bill was abandoned, mainly because the LGPD, like the GDPR, is extremely broad and goes beyond the scope of the internet.

Furthermore, as will be seen, the LGPD confers a more specific and practical application of rights to the data subject, which go beyond the mere judicial protection of rights that have already been violated. The intention of the LGPD is to regulate a stable relationship and prevent violations and abuses, and not to leave to the Judiciary the dispute resolution between the parties involved.

In any case, the LGPD has not yet entered into force and the provisions on personal data and privacy of the Civil Rights Framework for Internet have not been regulated, which means, mainly, that in Brazil the debate is not as advanced as in the European Union. Nevertheless, issues related to the use of artificial intelligence in the collection and treatment of data, as well as in the offer of products and promotions over the internet, are certainly a problem that we must face soon, with Brazil being the 5th largest nation in number of users of the internet on the planet[4].

Finally, and without intending to exhaust the matter, the LGPD may represent an important advance in the Brazilian legal framework in order to regulate the processing of personal data along the lines of the GDPR. There is no doubt that Brazil has a path to follow with regard to the culture of data protection. However, we believe that the entry into force of the LGPD can assist in raising civil society's awareness of the importance of having a clear rule that protects people and their data.

******

[3] Federal Law N. 12.965, of April 23, 2014.

[4] https://www.statista.com/statistics/262966/number-of-internet-users-in-selected-countries/. Access in April 13, 2020.

This report has been divided into two main parts: issues addressed in the light of already enacted legislation (positive law) and issues related to future developments or to points not expressly regulated by the law.

A) Issues in the light of enacted legislation

1. Search engines, artificial intelligence and freedom of contract.

A search engine is software designed with the aim of, upon an input by the user, searching the Internet for information and giving the result at the end. This search may use numerous tools that make it more efficient, such as the application of artificial intelligence, machine learning and other systems.

For the average user, understanding the intricacies of the mechanics employed in a search engine is often not feasible, especially if artificial intelligence is applied.

To further complicate the scenario, in addition to artificial intelligence technology, there is the application of "profiling" techniques, aiming to individualize the possible buyer based on the extraction of assumptions and predictions about his interests and behavior. However, the definition of a profile may be defective and suggest wrong information about the user, showing as results of his search products that do not correspond to his interests and expectations.

According to the ICO[5], "*As regards erroneous algorithmic decisions, there are clear implications for the data protection principle of accuracy, such as inaccurate predictions based on biased profiling*".

It is well-known that a contract denotes the need for a defined and well-specified object, in addition to the autonomy, civil capacity and free will of the parties involved. The human will, not the law, is typically the nucleus, the source and what legitimates a contractual relationship. The force that compels the parties to fulfill the contract is based on the will freely stipulated in the legal instrument, and the law is only responsible for ensuring the means that lead to the fulfillment of the obligation, thus having a supplementary position.

Should the search engine point the user to products that do not meet his/her expectations, it is possible to affirm that there is some mathematical / theoretical defect or simply insertion of erroneous data about the assumed profile of the internet user. Considering that the consumer uses a search mechanism (which may be vitiated) as a tool that leads him to find an object of desire, he may be induced to buy another object that is not fully compatible with his goals and needs. The end result would be a defect in the will of the

[5] https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf - Access in 27 April 2020.

user, who was erroneously led to close a deal he would not want if he was fully aware of the conditions of the search, results and offer.

By this logic, it appears that, in theory, the lack of knowledge of the underlying rationale of the search engine could suppress the consumer's contractual freedom by his/her being unduly induced to the acquisition of a certain product or service.

However, we believe that the claim that there is a presumed restriction to contractual freedom due to erroneous profiling lacks basis, since in addition to depending on the specifics of the case, a balance must be stroked between the rights of the user and the rights of companies related to trade and business secrets, equally protected by the LGPD, which may be the case in the way algorithms are programmed. In addition, due to the rapid advancement of technologies, there are now artificial intelligence structures that seek to rebalance this scenario, giving the choice back to the user.

In order to preserve the consumer, the Brazilian Consumer Protection Code[6] provides since 1990 that the offer of products and services must obey some rules, such as sufficient precision and clarity of information – including characteristics, qualities, quantity, composition, origin, price, risks to health and safety, among others -- and that any condition mentioned in an offer be included in the final agreement (articles 30 and 31)

The LGPD provides with regard to automated data processing that data subjects are entitled to request a review of decisions taken solely on the basis of automated processing of personal data that affect their interests, including decisions designed to define their personal, professional, consumer and credit profile or aspects of their personality (article 20). The article goes on to determine that the controller must provide, whenever requested, clear and adequate information regarding the criteria and procedures used for the automated decision, observing the commercial and industrial secrets. Failure to comply may cause na audit for discriminatory aspects in the automated treatment of personal data.

Therefore, granted that the legal provisions are respected, the mere misunderstanding of the logic of the search engines through artificial intelligence will not necessarily imply a restriction of contractual freedom, under penalty of rendering an important gain of society unfeasible in favor of a massive bureaucratization of business operations.

Notwithstanding the legal requirements and good practices related to the protection of personal data, which must be implemented and guaranteed to the data subject, it is essential to emphasize the importance of adopting an Artificial Intelligence Governance model integrated with algorithmic ethics, which inserts the individual as a protagonist in the management and development of automated analyzes. In this way, companies will be able - even if not completely - to guarantee to the data subject that the automatic decision-making process is the most transparent, balanced and consistent with the reality as possible.

[6] Federal Law No. 8,078 of 1990.

In order to accomplish this, according to the findings of Personal Data Protection Commission — Singapore PDPC, it is necessary for organizations to consider: (i) the adaptation or creation of their organizational governance structure, to incorporate related values, risks and responsibilities in the algorithmic decision-making; (ii) a methodology to assist them in defining their appetite risk for the use of artificial intelligence, that is, determining acceptable risks and identifying an appropriate level of human involvement in artificial intelligence decision making; (iii) issues related to the development, selection and maintenance of artificial intelligence models, including correct data management; and, finally, (iv) setting up communication and relationship strategies with stakeholders, mainly with the data subject.

Regardless of this fine balance between free will in contracting and the need not to hinder technological implementations in the market, there is another side to this issue. The matter of evaluating whether an advertisement based on the calculations of an algorithm does not match a consumer's interest is highly subjective – if not impossible in some situations.

First, because companies might not be able to publicly explain their algorithms' decisions due to industrial or trade secrets, which prevent them from sharing specific information about their algorithms' choices without a judicial order. Second, because some algorithmic decisions are unpredictable and caused by factors that companies cannot fully justify by what was intended at first place.

Third, stating that an advertisement exhibited due to algorithms' calculation is not equivalent to someone's whishes depends on a deep knowledge of this individual's interests, once one should be able to prove that the presented information does not correspond at all to his/her interests based on his/her previous behavior expressed online. Depending on the case, an algorithm may be highly sensitive to any input it receives, to the point that one different search performed by a consumer changes completely the ads that are depicted to him/her – especially in cases involving one same account used by different people.

If a customer presents a specific behavior online and suddenly changes it for any reason, it would be reasonable that algorithms took a period of time – which could be longer or shorter depending on the case – to adjust their calculations in order to filter information and depict ads that correspond to one's new interests – that could also be temporary wishes, following of trends, demanding temporary changes in the publicity material shown to the data subject.

On the other hand, it's also not reasonable to state that freedom of contract is unacceptably manipulated in this scenario, given that companies are presumably interested in offering services – and depicting ads - that best suit their customers' interests, to increase the chances of getting a deal closed. The companies in this case would gain nothing by violating their customers' contractual good faith. If a website invests in an algorithm that keeps showing users ads that do not correspond to what they are expecting, it would not achieve expected profits and would consequently make the website lose space to others platforms. Internet application providers seem to be more interested in drawing attention of people who share the same tastes and desires than to convince individuals that are not interested into their content.

For the above reason, it could be stated that there is less interest in manipulating a contract to exhibit advertisements that do not correspond to someone's wishes – through the programming of an algorithm - than in filtering the correct costumers in order to show them advertisements that would please each one of them specifically.

2. Lawful processing of data by chatbots (AI) upon closing of contracts

Article 6 (1) b of the GDPR provides that processing shall be lawful only if and to the extent that it is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.

This legal disposition has a perfect equivalent in the LGPD, article 7, item V.

In order for chatbots to be designed to lawfully process data under this legal disposition, it is necessary to consider the data subject's proactive action of "opening the call", in the sense of requesting help from the chatbot.

This tool will also need to be developed and based, essentially, on the principles of purpose, adequacy, necessity and transparency, as elucidated in Article 6, items I, II, III and VI of the LGPD.

That is, the information handled will need to be adequate and stick to the purpose that, in this case, is the performance of a contract. Likewise, there cannot be processing of data beyond what is necessary, in view of the principle of necessity, also known as "of minimization".

It is important to highlight that, in order to comply with the principles listed in the LGPD, it is essential that the controller - responsible for the treatment of personal data and who determines the purposes for which the personal data will be treated - adopts appropriate technical and organizational measures designed to internalize the principles of protection of personal data, integrating with new technologies, such as the chatbot, the principles of Privacy by Design, in order to guarantee privacy and the correct treatment of personal data not only from a regulatory point of view, but also from an organizational point of view, with the objective of extending privacy to the following, and comprehensive, triad: 1) IT systems, 2) commercial and business practices and 3) IT infrastructure.

This is precisely what Article 46, §2 of the LGPD provides, that is, the duty to adopt security, technical and administrative measures capable of protecting personal data from unauthorized access and accidental or unlawful situations of violation of personal data that must be observed from the product or service design phase until its execution. In this respect, a clear reference to privacy by design is perceived in the Brazilian law.

Finally, with the exception of issues pertaining to business secrets, the chatbot platform will need to be transparent regarding the treatment of data, especially if there is a possibility of transferring such data to third parties, in compliance with Article 9, item V of the LGPD.

Likewise, the National Authority (ANPD) may establish complementary rules for the activities of communication and shared use of personal data (Art. 30 of the LGPD).

Regarding the transparency principle, it is recommended that the platform uses a Data Protection and Privacy Policy that guides the data subject about how and for what purpose his data will be treated, the data retention period, who is the controller, in addition to responsibilities and rights, in compliance with Article 9 of the LGPD. As a good practice, a chatbot should use a clear and unambiguous language, aiming to interact with the user in a way that leaves no doubts about the functionalities and their reflexes about their personal data.

As there is still no operating authority, nor is there any jurisprudential or doctrinal guidance on the subject, Brazilian companies often resort to already consolidated understandings and guidelines from authorities in other countries.

3- Use of artificial intelligence for processing personal data and data protection impact assessment

Initially, it is important to clarify the concept of an Impact Assessment on the Protection of Personal Data (AIPD), called by the LGPD the Impact Report on the Protection of Personal Data (RIPD).

Both the GDPR and the LGPD provide that the controller must produce the RIPD when the data processing activities that are carried out represent risks to civil liberties and the fundamental rights of data subjects.

The RIPD, according to Art. 5, item XVII of LGPD is a documentation of the controller that contains the description of the processes of processing personal data that may generate risks to civil liberties and fundamental rights, as well as measures, safeguards and risk mitigation mechanisms. It is, therefore, "*a process that aims to establish risk mitigation mechanisms and demonstrate regulatory compliance, through a document*"[7].

The main difference between the GDPR and the LGPD as regards this kind of report is that the GDPR establishes occasions when the impact evaluation is mandatory, whereas the LGPD, at least in a literal

[7] LGPD Acadêmico. "Relatório de Impacto à Proteção de Dados Pessoais", p. 14. Link: http://wix.to/-UDYBak. Access in 26 April 2020.

interpretation, establishes that such a report is only needed when the National Authority demands it (art. 10, §3 and art. 38).

This fact, however, in no way prevents nor should discourage companies, organizations and entities from maintaining a proactive stance and, based on international best practices, produce their respective Impact Reports in advance of any request by the National Authority, whenever the activity at hand can represent a risk to individual freedom and rights. It is worth mentioning that the proactivity of companies in relation to risk mitigation is an important aspect of the dosimetry of possible fines and other reprisals provided for by law in an alleged event of data leakage, as established in Article 52, § 1 of the LGPD and its items, in special the good faith of the infringer (item III), the reiterated adoption of internal mechanisms and procedures capable of minimizing damages in the treatment of data (item VIII) and the general adoption of a policy of good practices and governance (item IX):

By adopting this measure, organizations will be complying with the principle of accountability, provided for by both European regulation and Brazilian legislation, which consists, as provided in Article 6, X of the LGPD, in the demonstration, by the agent, of the adoption of effective measures capable of proving the observance and compliance with the rules of protection of personal data, including the effectiveness of these measures.

Under the LGPD, the use of artificial intelligence to process personal data in order to control the interaction with the data subject will be susceptible to the production of a Personal Data Protection Impact Assessment whenever it may imply a high risk to the data subject, which may generate risks to civil liberties and fundamental rights, especially when (i) the processing is based on legitimate interest or (ii) when sensitive data is processed.

Finally, Working Party 29 - an independent European working group that, after the entry into force of the GDPR, was replaced by the European Data Protection Board (EDPB) spoke on the issue through guidelines issued on April 4, 2017, which were endorsed by EDPB, regarding the Impact Assessment on Data Protection. The legal opinion establishes 09 (nine) criteria that must be observed for the elaboration of a RIPD and, among them, two apply to the case at hand, which is already sufficient to justify the spontaneous adoption of the referred procedure, namely: (i) systematic control by data subjects through (ii) innovative solutions or application of new technological solutions.

4- AI software, individualized advertising and the lawful processing of data under the “legitimate interest” clause

LGPD Art. 7, item IX, establishes that the processing of personal data can only be carried out when necessary to serve the legitimate interests of the controller or third party, except in the event that the fundamental rights and freedoms that require the protection of personal data of the data subject prevail. This article is very close to what article 6 (1) f of the GDPR establishes.

The legality of an artificial intelligence software combined with the tracking of cookies for the purpose of individualized advertising will be, as determined by art. 10, items I and I and §§ 1st and 2nd, directly conditioned to (i) serving the legitimate interests of the controller or third parties, which may include supporting and promoting the activities of the controller; (ii) the treatment of data that is strictly necessary (necessity and minimization); (iii) with respect to the data subject's legitimate expectations and fundamental rights; (iv) with the adoption of measures to guarantee the transparency of the treatment.

Finally, as already mentioned, according to Art. 10, § 3 of the LGPD, the national authority may request from the controller an impact report on the protection of personal data, when the treatment is based on its legitimate interest, observing commercial and industrial secrets.

Therefore, there is the possibility that this type data processing takes place in accordance with Brazilian law; however, the controller must carry out an assessment on the treatment to confirm that it is based on a legitimate interest and to use administrative and technical measures of information security to protect the data subject.

Controller should also be transparent about the treatment of data and allow the data subject to opt out of receiving such advertisements, as a measure of good market practice and in line with the Consumer Protection Code. Depending on how personalized pricing/content / advertisements play out after the LGPD enters into force, the ANPD may make the use of labelling of personalized content and opt-out clauses mandatory in order to guarantee enforcement of the law and its goals and principles.

5. Profiling and individualized ads and prices under the LGPD

Upon tackling this issue, it is worth mentioning that LGPD does not have an article corresponding to Art. 22 (1) of the GDPR on individual automated decisions, including definition of profiles, which provides that “the data subject has the right not to be subject to any decision taken exclusively based on automated treatment, including the definition of profiles, which has an effect on its legal sphere or which significantly affects it in a similar way. ”

However, as already stated, the LGPD does establish in its article 20 that the data subject has the right of requesting the review of decisions taken based on the automated treatment of personal data that affect their interests, including his profiling.

There is a subtle difference between having “the right not to be subject to any decision" (GDPR) and having the right to request review of decisions already taken (LGPD). In the first case, the exercise of the right implies that the data subject will not be subject, having made an option in this sense, to any automated decisions, whereas in the text of the Brazilian law this subjection will occur despite the data subject, but the decisions already taken may be subject to review at the request of the data subject.

Another aspect that deserves to be highlighted is the fact that it is not clear in Art. 20 of the LGPD how an automated decision will be reviewed. This circumstance deserves attention because, when considering the legislative changes proposed by the Brazilian National Congress by means of Law N. 13,853/2019, which altered some articles of the LGPD, the President of the Republic decided to veto the article that established that this review must be done by a human being.

Therefore, the review referred to in that article, when requested by the data subject, may be redone by exclusively automated means, without any human verification.

To the extent that there is a decision made solely on the basis of automated processing of data that affects the interests of the data subject, including decisions designed to define his personal, professional, consumer and credit profile, or even aspects of personality, the data subject may:

> (i) Request a review of this decision, which may likewise be carried out using automated means; and
>
> (ii) Request from the controller information on criteria and procedures, observing commercial and industrial secrets. If the controller does not provide them, the national authority may perform an audit to verify discriminatory aspects in automated processing of personal data.

However, Brazilian law lacks specific regulation by the ANPD, which is not yet constituted. Thus, there is still no precedent that establishes parameters for the interpretation of that specific article.

In view of the absence of specific regulations in Brazil, it is worth mentioning the definition of "profiling" in Article 4 (4) of the GDPR: the automated process used by the controller of personal data in its possession, aiming to extract assumptions and predictions about certain aspects of a person, such as his performance at work, economic situation, health status, personal preferences, interests, behavior and other personal aspects.

It is important to understand that the practice of creating prices and personalized advertisements is extremely dependent on the results of the profiling process, and the extraction of personal presumptions from the natural person are the raw material for this practice.

According to Mendoza e Bygrave[8], certain aspects must be present in the process for article 22 of the GDPR to be applied, namely: (i) the existence of a decision, based solely and exclusively on automated data processing, by means of any technique that does not involve human intervention, including the

[8] Mendoza, I., & Bygrave, L. A. (2017). The Right Not to Be Subject to Automated Decisions Based on Profiling. In T. Synodinou, P. Jougleux, C. Markou, & T. Prastitou (eds.), EU Internet Law: Regulation and Online Price Discrimination and EU Data Privacy Law 365 Enforcement. Springer, 2017, Forthcoming; University of Oslo Faculty of Law Research Paper No. 2017– 20: In <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855>. Access on April 22, 2020.

practice of profiling and (ii) that the decision causes legal or significantly relevant effects to the target person.

In the case of personalized prices, article 22 is applied whenever an algorithm (i) decides automatically an individualized price for a customer and (ii) the results extracted from the application of that algorithm are used to evaluate and measure the customer's personal aspects in theory, such as his/her willingness to buy a particular item, as well as his/her economic situation.

These two conditions denote the existence of an individualized price that results directly from an automated processing of personal data.[9].

It is necessary to mention that, in the case of the existence of automated decisions, including the definition of profiles, the European regulation requires a kind of "extra transparency", since Article 13, 2, F and Article 14, 2 , F of the GDPR establish that the controller must provide useful information regarding the underlying logic of profiling, as well as the importance and expected consequences of such treatment for the data subject. The criteria and timing for providing this information vary depending on whether or not the personal data is provided directly by the data subject. In the negative case, the controller must inform the origin of the personal data obtained and, if necessary, whether such data comes from publicly accessible sources.[10].

In view of the above, within the scope of the LGPD, the creation of personalized advertising or personalized prices generated based on decisions taken solely from the automated processing of personal data that affect the interests of the data subjects should give the data subject the right of review of such decisions, a review which can also be automated, as well as the right to gain knowledge about the criteria and procedures used for the automated decision. In the event of non-availability of information that does not constitute commercial and industrial secrets, the ANPD may perform an audit to verify discriminatory aspects (eg price discrimination) in the automated treatment of the personal data in question, without prejudice to sanctions arising from consumer and antitrust law.

6 – (In)sufficiency of the instrument of informed consent to data processing

The fact that the consent is just "informed" is not enough to protect the consumer / data subject under Brazilian Law. This is because consent must be composed of other essential attributes that are inherent to its validity.

[9] Online Price Descrimination and EU Data Privacy Law, Frederik Zuiderveen Borgesius e Joost Poort. Access in <https://link.springer.com/content/pdf/10.1007/s10603-017-9354-z.pdf> April 22, 2020.

[10] According to the GDPR, the controller must provide data subjects with concise, transparent, intelligible and easily accessible information on the processing of their personal data. For data collected directly from the data subject, this must be provided at the time of collection (article 13) and for data obtained indirectly, the information must be provided within the time limits established in article 14.

According to “Recital 32” of the European Regulation on the Protection of Personal Data, consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data subject’s agreement to the processing of personal data relating to him or her.

Therefore, it is clear that, in order to be considered valid, consent must be granted by the data subject in a proportional and balanced relationship, a fundamental requirement for compliance with the “freely” attribute.

Furthermore, for the consent to be “specific”, the purposes of the processing of personal data must be very clear to the data subject, so that there is no doubt about the purpose(s) of treatment to which the data subject is consenting.

Still in relation to the fundamental characteristics and inherent to the validity of the consent, it must be “informed” to the data subject, therefore, the specifics of the personal data processing operations must be very clear and transparent to the data subject so that, when informed of the purposes, he or she can consent from an affirmative and unambiguous stance. Therefore, there is no such thing as a tacit consent or consent by omission. To the thesis that consent must be “informed” underlies the obligation that the tools involved in the process of getting such consent must be explained in clear and unambiguous language, aiming to give the data subject the correct and faithful “portrait” of the dynamics to which his or her personal data will be subject.

Besides Recital 32, article 7, 1 of the GDPR establishes that where processing is based on consent, the controller shall be able to demonstrate that the data subject has consented to processing of his or her personal data.

Therefore, the controller must seek ways to collect the consent that are able to demonstrate the veracity of the concession made by the data subject so that, in this way, it fulfills the last and indispensable attribute fo consent, which is to be “unambiguous”.

All attributes, therefore, seek to rebalance the relationship between the agents of personal data processing and the data subject. Conversely, the data subject would find himself in an extremely unfavorable position to understand the purposes of the data processing activities.

Article 5, item XII of the LGPD establishes consent is the free, informed and unequivocal manifestation by which the data subject agrees with the treatment of his personal data for a specific purpose.

Therefore, in the same way as the GDPR, Brazilian law aims to bring greater security to the activities of processing personal data carried out based on consent, not allowing the hypothesis of a too wide and too general consent, whose treatment is not assigned to a specific purpose and to which the data subject has not granted consent freely and unequivocally, under penalty of being considered void due to defect of consent (Art. 8 § 3, § 4 of the LGPD).

In addition, the treatment agent must use the means to operationalize the consent and the duties that emanate from it, considering the legal possibility of the consent being revoked at any time by the data subject and the fact that the burden of proof that the consent has been lawfully obtained will be borne by the controller (Art. 8, § 2 and § 5 of the LGPD).

Such requirements were legally established in order to guarantee to the data subject the due proportionality and harmony in the treatment relationship, transparency and clarity in the provision of information and affirmative and unequivocal mechanisms of actions, by the data subject, for specific and agreed purposes, in order to enable the controller to prove that it has lawfully collected consent.

Finally, both regulations aim at promoting the restructuring of the current model of concession and generic authorization for the activities of processing personal data, resuming the necessary and fundamental balance between the processing agents and the data subjects. This is undertaken especially bearing in mind the current difficulty of the data subjects in understanding extensive and complex Privacy Policies and technical intricacies of technology, programming and other technical aspects.

One of the best ways to operationalize consent, guaranteeing all the attributes inherent to its validity, is through "*visual law*"[11], linked to granularized consent, which allows greater legal certainty to the two poles that are part of the same personal data processing relationship: the processing agent, who requires consent, and the data subject who grants consent to the use of the data for a certain purpose.

7 – Consent, cookie policy and access to services rendered on the internet

Article 7 (4) of the GDPR establishes that conditioning the execution of an agreement or rendering of services to consent for treatment of personal data is only acceptable when this treatment is strictly needed for the rendering of services or execution of the agreement.

The LGPD does not bring an article with the same content or at least similar to the parameters set in Recital 43 of the GDPR. An integrated interpretation of the principles set out in the LGPD is needed to reach the same effects of Article 7 (4) of the GDPR.

According to the LGPD, consent is defined as "free, informed and unambiguous expression by which the data subject agrees with the treatment of his personal data for a given use" (Art. 5, XII).

However, when the processing of personal data is based on the performance of an agreement, the controllers will not be able to condition the contractual performance to the consent of the data subject, for

[11] https://www.jusbrasil.com.br/topicos/241689619/visual-law?ref=doc-topics. Access in 23 April 2020.

the processing of additional personal data, other than those effectively needed to achieve the purpose of the agreement in question. This interpretation results from the application of the principles of necessity and purpose. The principle of necessity imposes the limitation of treatment to the minimum necessary for the realization of its purposes, with the scope of relevant data, proportional and not excessive in relation to the purposes of data processing (Art. 6, II). In turn, the principle of purpose provides for “the treatment to be carried out for legitimate, specific, explicit and informed purposes to the data subject, without the possibility of further treatment in a manner incompatible with these purposes” (Art. 6, I).

At the end of the day, we can say that it will be up to the scholars, jurisprudence or the National Data Protection Authority (ANPD) to establish an interpretation parameter.

With regard specifically to the LGPD, there is no jurisprudence in this regard, as the law is not yet in force, nor has the ANPD been established.

Despite the lack of jurisprudence on the subject, it must be said that it is still common for Brazilian companies to adopt privacy policies in a global and generic way, in which the data processing is “fully accepted”, without the necessary request for granular consent for the processing of personal data. However, LGPD prohibits the practice of generic and overly comprehensive policies, by providing that "consent must refer to specific purposes, and generic authorizations for the processing of personal data will be null" (Art. 7, § 4). We emphasize that there is a gradual mindset and cultural change underway, on the part of treatment agents in Brazil, to adapt their privacy policies to this requirement.

As much as the Brazilian rule expressly prohibits the processing of personal data by means of a defect of consent (Art. 7, § 3), this device still depends on specific regulations, which will eventually be formulated by the competent authority.

In this regard, the guidance of the Information Commissioner’s Office (ICO) and Recital 43 of the GDPR is welcomed.

According to Brazilian law, if the use of any tool on the site is subject to the treatment of certain personal data, the data subject will have the right to receive this information in a prominent way. If the data subject does not provide consent, the processing agent must inform him about the consequences of this refusal, in accordance with articles 9, paragraphs 3 and 18, item VIII of the LGPD.

There is no formal norm or parameter in Brazil, but some Brazilian companies have been adopting the guidelines of international organizations in their preparation processes for adaptation to the LGPD. Thus, one of the most interesting parameters is that contained in the already mentioned guide provided by the Information Commissioner’s Office in the United Kingdom - ICO. According to such guidance, the user must have full knowledge of the cookie technologies, or any other with the function of collecting and storing personal information through the websites.

In addition, the aforementioned technology and its reason for use must be clearly explained, even though the information collected and processed is anonymous, being necessary, in most cases, to obtain the user's consent in a clear, specific and unambiguous way.

In addition, according to the European Data Protection Board, there are two exceptions to the use of cookies without the user's express consent being required. The first is when cookies are used to help, speed up or regulate the transmission of communication between services in the "electronic communications network" system, as long as communication is not possible without the use of cookies. The second is when cookies are strictly necessary for the activation of a service required by the user, that is, with cookies disabled, the service would not work.

Considering the time lapse between the publication of the LGPD and its entering into force, as well as the absence of regulation and guidance by the ANPD, there are currently no objective answers to issues that are somewhat only potential. However, our comments above reflect current trends and practices already adopted by some companies to (i) obtain granular consent, when necessary; and (ii) do not make the use of websites subject to the provision of consent, except when data subject to consent is strictly necessary for the effective rendering of the service.

8 – Black box phenomenon and the transparency principle

The "Black Box" Phenomenon is typically noticed in the realm of artificial intelligence, since it is due to the developers' lack of understanding about the underlying principles and parameters of decision making of devices with artificial intelligence.

Artificial intelligence algorithms consist of a set of mathematical rules that will automate a process previously performed by a human. So, technology, in fact, does not change reality, but rather enhances the context of reality that already exists, and automates the "status quo", since the initial data, that bring the machine's purpose and learning process to life, may have a bias in terms of neutrality, presenting themselves, albeit in a subtle way, as biased data.

Considering that the set of mathematical rules inserted in the machine is essentially consisted of business secrets, it is possible to infer that the principle of transparency may have its efficiency suppressed in practice. However, there are already frameworks issued by Personal Data Protection Authorities that aim to guide a governance model in technologies such as artificial intelligence, in order to guarantee the rights of data subjects and mitigate risks that involve the treatment of their information. This is the case, for example, of the Personal Data Protection Commission of Singapore (PDPC), which issued guidelines on the subject on January 21, 2020.[12].

[12] Personal Data Protection Comission – PDPC. Model AI Governance. Link: https://www.pdpc.gov.sg/model-ai-gov. Access on April 26, 2020.

According to the model suggested by the PDPC, organizations that use artificial intelligence should:

(i) ensure that the decision-making process is explainable, transparent and fair; and

(ii) place individuals, data subjects, as the main driver of technology, that is, centralize the individual in the development of the solution, aiming to protect individual rights, promoting their well-being and their security.

There is, of course, a possibility that the system will be able to demonstrate to the user the process that resulted in the decision, however, this demand constitutes a notable challenge for the LGPD due to the provisions of the final part of Art. 6, VI, which conditions transparency to the safeguarding of commercial and industrial secrets.

That said, p*rima facie*, the black box phenomenon is not compatible with the transparency principle of the Brazilian General Personal Data Protection Law (the "LGPD").

The transparency principle means that processing agents shall provide data subjects with clear, accurate and easily accessible information about the personal data processing, including the processing chain of agents. Therefore, in order to be compatible with the transparency principle, data subjects need to have easy access and, in fact, understand information about the decision-making processes of the artificial intelligence. However, considering that the algorithmic decisions are usually characterized by opacity, it is not an easy goal to achieve, in practice, even in relation to supervised machine learning, in most circumstances.

Article 20 of the LGPD, already cited in this report, establishes that data subjects are entitled to request the review of decisions taken solely based on automated processing of personal data that affect their interests, including decisions designed to define their personal, professional, consumer and credit profile or aspects of their personality. Article 20, paragraph 1 institutes the right to explanation, derived from the transparency principle, determining that the controller must provide data subjects, whenever requested, with clear and adequate information regarding the criteria and procedures used for the automated decision.

The LGPD does not estipulate the same exceptions provided in the GDPR regarding the non-applicability of the duty to provide information about the existence of automated decision-making and the meaningful information about the algorithms' logic and the envisaged consequences of such processing for the data subjects. Thus, the LGPD seems even more severe than the GDPR in this aspect. On the other hand, Article 20, paragraph 2 of the LGPD establishes that if the controller evokes commercial and industrial secrecy as a justification not to present such information, the ANPD may carry out an audit to verify discriminatory aspects in automated processing of personal data. Such audit has not been regulated by the ANPD yet.

In view of the complexity of the artificial intelligence decision-making process, an interpretation in the sense that there is a prohibition on the use of machine learning algorithms whose decision-making activity are inscrutable could result from Article 20, paragraph 1 of the LGPD. However, such solution would be counterproductive and not feasible from an economic standpoint.

Alternatively, transparency can be interpreted under two aspects: (i) accessibility and (ii) understandability[13]. Accessibility, interpreted as providing access to the program source code, may not be sufficient to provide explanation about the automated decision making, since the source code only exposes the machine learning method used, and not the decision parameters. On the other hand, the understandability about the criteria[14] used for the automated decision is quite desirable.

In general, algorithms can be understood when the human being is able to articulate the logic of a specific decision (without the need to know the details of how the system achieved the decision). Therefore, in order to eliminate or at least reduce the black box phenomenon in a way to make the decision-making processes of the artificial intelligence compatible with the transparency principle, it might be necessary to apply technical and entrepreneurial efforts supported by public policies in the conception of the algorithms, such as to[15]:

(a) train AI systems with human-interpretable terms and store data from each decision in order to probe the decision afterwards;

(b) establish different levels of controllability according to the different machine learning methods (*i.e.* supervised, unsupervised and reinforcement learning) and techniques (*e.g.* semantic networks and natural language processing, regression analysis, artificial neural networks, etc.);

(c) prefer the adoption of machine learning methods and techniques that facilitate control and understandability, allowing for the artificial intelligence algorithms to use more complex logic only for a few cases that really need it (balancing transparency and business performance); and

(d) design updatable AI systems to train proxies to verify whether predictions of terms that cannot be determined in advance through the learning inputs (such as in a litigation process) are correlated with the automated decisions generated by the AI system.

[13] MITTELSTADT, Brent Daniel et al. The ethics of algorithms: Mapping the debate. Big Data & Society, 1-21, jul.-dez. 2016. https://journals.sagepub.com/doi/full/10.1177/2053951716679679. Access in April 22, 2020.

[14] The criteria would be: (i) what are the main factors that led to the decision; (ii) whether changing any of the determining factors would change the decision; and (iii) analyzing whether similar cases had different decisions and determining processes. see FERRARI, Isabela. *Accountability de Algoritmos*: a falácia do acesso ao código e caminhos para uma explicabilidade efetiva. Available at: <https://itsrio.org/wp-content/uploads/2019/03/Isabela-Ferrari.pdf>. April, 22, 2020.

[15] These comments are made under the assumption that, in most cases, it is technically feasible to extract the kinds of explanations that are currently required of humans from artificial intelligence systems.

In Brazil, there are already initiatives for the establishing of large shared and open databases (Serenata.ai and Colaboradados) so that different algorithms can use them in their training, allowing biases can be identified and corrected by everyone.

The use of machines is expected to eliminate the prejudices or subconscious processes that affect human thought or, at least, to enable us to recognize them more easily whenever they appear.

9 – On the legality of manufacturers' prohibition of the sale of their products on certain platforms in order to protect the product's image[16]

According to Article 132, III of the Brazilian IP law, the trademark owner may not restrain the free circulation of products placed on the internal market by himself or by another with his consent. Such order is related to the principle of the exhaustion of trademark rights, which states that the trademark owner may not invoke exclusivity in order to restrain subsequent sales, after the first sale of a product on the market.

On Adcos v. Mercado Livre, the São Paulo Court of Appeals[17] rejected the Plaintiff´s appeal in order to restrain the Defendant from disclosing Adco´s products on its platform, which was being sold by third parties. The 06th Chamber of Private Law ruled that the trademark owner may not justify its prohibition claim under the argument of protection of its product´s image, since it is underpinned on future and uncertain damages that, if occur, can be later repaired. Moreover, according to such decision, "*the supplier is liable for the ensuring of the safety of the product it places on the market, which should also consider the possibility of reselling the product after the exhaustion of trademark rights*".

It is worth highlighting that, between the supplier and distributor, nothing prevents the supplier from, on contracts that have exclusive or selective distribution clauses, prohibiting its distributors from selling its products on certain platforms, such as in marketplaces. Thus, in a contractual sphere between supplier-distributor, Brazilian law does not forbid such prohibition.

However, once these official distributors launch the supplier´s product on the national market, there is no way to prevent the free resale of this products by any third party, including on e-marketplaces. This understanding was adopted by the Superior Court of Justice, on Citizen Watch v. Mercado Livre[18], in which the Rapporteur Minister emphasized that drastic measures to control internet content should only

[16] Our analysis does not include comments with respect to the purchase of keywords, by distributors, containing trademarks for the sale of their products.

[17] Lawsuit # 0031284-65.2013.8.26.0068 – Adcos Indústria e Comércio LTDA vs. MercadoLivre.com Atividades de Internet Ltda. 06th Chamber of Private Law, Rapporteur Judge Eduardo Sá Pinto Sandeville. Court of Appeals´decision issued on March 22, 2018.

[18] Lawsuit # 1.383.354 – SP – Citizen Watch do Brasil S/A vs. MercadoLivre.com Atividades de Internet Ltda e Outro. Third Pannel, Rapporteur Minister Nancy Andrighi. Superior Court of Justice´s decision issued on August 27, 2013.

be used in extreme cases, and should not be adopted as a rule, especially in the case of individual interests, without great serious risk of damages.

In specific cases in which effective damages are verified, although the trademark owner can file a lawsuit seeking compensatory damages against the liable party, the online platform itself cannot be liable for such practices. As duly mentioned on our Report of 2018[19], internet application providers will only be held liable if, after a Court decision, they fail to take action to make unavailable the infringing content, as set forth by Article 18 and 19 of the Civil Rights Framework for Internet.

This said, under Brazilian law it is illegal for manufacturers to prohibit distributors from advertising the manufacturer's products on search engines inasmuch as the trademark owner does not have limitless rights regarding the trademark use.

Brazil has an important precedent about this issue, applying this exception to cases of sponsored links, in the case of L'Oréal vs. Beleza.com (Interlocutory Appeal # 0089493-71.2012.8.26.0000; 1st Reserved Chamber of Business Law of the São Paulo Court of Justice, judgment date: 6/1/2012). The Court has ruled that "it is legal to use the adwords tool to promote the sale of products made available to consumers on the websites of distribution companies"[20].

The Brazilian Superior Court of Justice also decided in September 13, 2016 (Special Appeal # 1.606.781/RJ) that, in cases involving sponsored links, the mere mention of the registered trademark on search engines is not considered as unfair competition. Therefore:

a) the owner of a trademark cannot prevent it from being used by the distributors, and placed together with distributor's trademark, when there are legitimate promotional or commercial purposes for original products and / or services;

b) in such cases of promotion and commercialization of the trademark owner products on their physical establishment commerce or over the Internet, it is not necessary for the distributors to obtain an authorization, in view of the fair use exception referred above.

Notwithstanding, even in the context of promotion and commercialization by distributors, the use of the trademark is bound to some restrictions. It means that the trademark cannot be used in an unrestricted/indiscriminately way, without any limitation and upon the distributor's own criteria, or used to boost that distributor's business prominently. The use of trademarks by distributors in advertising the manufacturer's products on search engines must be justified and loyal.

[19] See also our past report solely on this subject in Chapter 17 of Këllezi, et.al. *Liability for Antitrust Law Infringements & Protection of IP Rights in Distribution*. Springer: Cham, 2018.

[20] https://tj-sp.jusbrasil.com.br/jurisprudencia/22004983/agravo-regimental-agr-894937120128260000-sp-0089493-7120128260000-tjsp/inteiro-teor-110494544?ref=juris-tabs

The distributors must make it clear to the public that they only sell the product, but they are not a trademark licensee or there is no commercial relationship with the trademark owner, aside from distribution, so as not to constitute unfair competition.

In this sense, it is important to emphasize some relevant aspects so that it may be considered a fair use according to the IP Law:

(i) the trademark owner may verify the real context of the trademarks that are used by the distributors when adverting its products on searching engines,

(ii) the trademark owner may analyze if there is an intention of the distributor to cause confusion or undue association with the true owner to mislead consumers, for example, when the distributor uses the trademark owner's logo, the same fonts and/or colors of the legitimate trademark owner, making an evident allusion to the owner's logo or its website layout.

(iii) the distributor may not use the trademark to try to misrepresent that it has a business relationship or association with the trademark owner and the use is allowed as long as the standards set forth by the trademark owner are followed by the distributors, in order to avoid unfair competition or violate the trademark owner rights set forth on article 129 cited above; and

(iv) the distributor of accessories that are used or compatible with a third party product and/trademark may not try to obtain undue advantage by misrepresenting that his accessories are manufactured or endorsed by the trademark owner of the main product. For example, the distributor cannot imply that its accessory is originated from or that it refers to the original product manufacturer.

10 - Unequal competitive conditions and the use of artificial intelligence by businesses.

Artificial Intelligence is a challenge in every single sector of the economy, due to the unavoidable growth of its use owing to the benefits it can provide, such as long term savings to the companies' budgets - despite the expensiveness of its implementation in a short term -, and celerity and improvement to its most varied processes. Truth is that the use of artificial intelligence is not forbidden in the Brazilian legislation, including Brazilian Competition Law. What will define if the company acts in compliance with the law or not is not the simple use of this technology itself, but the purpose for which it uses the artificial intelligence and the means of obtaining the data for the artificial intelligence models. It is undeniable that we all will be left behind by the artificial intelligence if we do not find a way to adapt to this technology, and the same applies to companies that are capable of operating with artificial intelligence mechanisms and technologies, that will certainly have better competitive conditions, and cannot be prevented from doing so as long as they comply with the law.

So, it is beyond doubt that employing IA in services will give a competitive edge to companies and it is likely that doing so will not be deemed a *per se* infringement, at least from a current law point-of-view. How crucial AI will be in the future and the proportions of this competitive edge, however, may lead to added government control in companies' affairs to curb undue market control, from decisions considering AI technologies an essential facility on some segments to regulations which determine sharing of AI technologies through a network of regulated companies.

11 – Algorithms and discrimination against companies in the placement of new advertisements.

One of the main purposes of algorithms is filtering and ranking information based on factors included in their code, due to the numerous data online and the limited capacity of an individual to absorb it all. They are essential in a society that requires the organization of the information received according to what would be more relevant to one person.

In this regard, algorithms that evaluate previous purchase decisions and then place new advertisements would not aim at deleting or hiding information or benefiting any company for unreasonable motivations – which would constitute a discriminatory practice. Basing new advertisements to be received by consumers on previous purchase decisions seems a rational type of ranking, especially considering they are intended to be personalized according to one's interests.

Despite the fact that this type of algorithm could make it more difficult for new businesses or struggling companies to stand out, it does not prevent them from having their advertisements exhibited to consumers in a proportional form according to their sales – even if in a less frequent way compared to others. Also, these companies might address other kinds of marketing strategies, increasing their purchase numbers, which will enable them to start being considered by the described algorithms (again).

Of course, depending on the spread of use of algorithms that place new ads based on previous purchase decisions by consumers/ data subjects, eventual intervention in the market may be needed in order to avoid the tunnel effect that could ultimately exclude new businesses. In other words, while the possibility is there, the current situation does not allow us to conclude that an intervention in the market to curb the activity of these types of algorithms is necessary or urgent.

B) Issues in the light of legal principles and propositions for future regulation

1 – Transparency and automated data collection

It is known that oftentimes the collection of data by artificial intelligence escapes the control of the companies that set the AI, resulting in the controller not knowing what data from third parties is ultimately being collected. This could affect the transparency principle, which, as already referred in this report, is one of the guiding principles of the LGPD as well as of the GDPR.

In these cases, it is recommended to adopt one or more of the best practices to ensure the safety of Internet users regarding personal data processing activities, namely: (a) insertion of privacy notices on websites (banners) that information about the collection of data user's personal data; (b) insertion of Privacy Policy and Cookies Policy with clear and accessible language; and (c) inserting the link of the third party privacy policy that has access to the data collected on the website in the privacy notices and / or policies of the website.

In addition, it is important to mention that the Civil Rights Framework for the Internet establishes in its article 15 that providers of Internet applications, constituted in the form of legal entity and that exercise this activity in an organized manner, professionally and for economic purposes, must keep records of access to their applications for a period of 6 (six) months, counted from the date of access to such applications.

Thus, even if the controller does not know exactly what third party data is collected on his website, it is possible to infer that, due to a legal obligation, his website collects, at least, the records of access to his applications (the set of information referring to the date and time of use of a given internet application from a given IP address). Therefore, in the privacy notices and / or Privacy Policy of the website, the need for such collection of personal data must be stated.

2 - Need of additional legal instruments to restrict the collection and use of data for the personalization of content/advertising/prices

With the entry into force of the LGPD, the processing of personal data in Brazil [21] can only occur in one of the 10 (ten) cases provided for in article 7, for "common" personal data[22], or in the 08 (eight)

[21] According to article 5 of the LGPD, treatment of personal data is defined as "any operation performed with personal data, such as those referring to the collection, production, reception, classification, use, access, reproduction, transmission, distribution, processing, filing, storage, elimination, evaluation or control of information, modification, communication, transfer, diffusion or extraction ".

[22] Art. 7 The processing of personal data can only be carried out in the following cases:
I - by providing consent by the data subject;
II - for the fulfillment of a legal or regulatory obligation by the controller;
III - by the public administration, for the treatment and shared use of data necessary for the execution of public policies provided for in laws and regulations or supported by contracts, agreements or similar instruments, subject to the provisions of Chapter IV of this Law;
IV - to carry out studies by a research body, guaranteeing, whenever possible, the anonymization of personal data;
V - when necessary for the execution of a contract or preliminary procedures related to a contract to which the data subject is a party, at the request of the data subject;
VI - for the regular exercise of rights in judicial, administrative or arbitral proceedings, the latter under the terms of Law No. 9,307, of September 23, 1996 (Arbitration Law);
VII - for the protection of the life or physical security of the data subject or of a third party;
VIII - for the protection of health, in a procedure carried out by health professionals or by health entities;
VIII - for the protection of health, exclusively, in a procedure performed by health professionals, health services or health authority;

hypotheses described in article 11[23], for sensitive personal data, i.e., personal data about racial or ethnic origin, religious belief, political opinion, union membership or organization of a religious, philosophical or political nature, data relating to health or sexual life, genetic or biometric data, when linked to a natural person[24], which is the main type of data collected and treated for the personalization of content, advertising and prices.

As a rule, the use of such hypotheses (legal bases) of treatment does not require that those responsible for the processing of personal data prepare other documents to guarantee the rights of the data subjects, except the notices and privacy policies that provide transparency to users about the activities of processing of personal data.

However, the hypothesis of the legitimate interest of the company responsible for processing (controller) or third party, provided for in item IX of article 7, can be conditioned to the issuance of another legal document, namely, the Impact Report on the Protection of Personal Data ("RIPD")[25], a documentation of the controller containing a description of the procedures for processing personal data that may generate risks to civil liberties and fundamental rights, as well as measures, safeguards and risk mitigation mechanisms[26], which may be requested by the Brazilian Data Protection Authority when the legitimate interest is used as a legal basis for the processing of personal data.

It should also be noted that, inspired by the recommendations of the European Union's data protection authorities and while the Brazilian Data Protection Authority is not, in fact, constituted, the Brazilian market has chosen to carry out a balance test between the interests of the controller and the rights of data subjects (Legitimate Interest Test) to analyze and minimize the impacts on the privacy of the data subject.

IX - when necessary to serve the legitimate interests of the controller or third party, except in the event that the fundamental rights and freedoms of the owner prevail that require the protection of personal data; or

X - for credit protection, including the provisions of the relevant legislation.

[23] Art. 11. The processing of sensitive personal data can only occur in the following cases:

I - when the data subject or his legal guardian consents, in a specific and prominent way, for specific purposes;

II - without providing consent from the data subject, in the cases in which it is indispensable for:

a) compliance with legal or regulatory obligations by the controller;

b) shared treatment of data necessary for the execution, by the public administration, of public policies provided for in laws or regulations;

c) carrying out studies by a research body, guaranteeing, whenever possible, the anonymization of sensitive personal data;

d) regular exercise of rights, including in contract and in judicial, administrative and arbitration proceedings, the latter under the terms of Law No. 9,307, of September 23, 1996 (Arbitration Law);

e) protection of the life or physical safety of the data subject or of a third party;

f) protection of health, in a procedure carried out by health professionals or by health entities; or

f) health supervision, exclusively, in a procedure performed by health professionals, health services or health authority; or

g) guarantee of fraud prevention and security of the data subject, in the processes of identification and registration authentication in electronic systems, safeguarding the rights mentioned in art. 9 of this Law and except in the event that the fundamental rights and freedoms of the data subject prevail that require the protection of personal data.

[24] Article 5, item II of the LGPD.

[25] Article 10, paragraph 3 of the LGPD.

[26] Article 5, item XVII of the LGPD.

In view of the above, the combination of the dispositions of the LIPD and an adoption of a proactive stance with the application of a test of balance of interests seems to be sufficient to avoid the need of additional legal instruments to restrict the collection and use of data for the personalization of content/advertising/prices.

3 –Creation of user profiles which currently also use data from international third party sources

In Brazil, there is no restriction on the processing operation that involves personal data from outside the national territory and that are not the object of communication, shared use of data with Brazilian processing agents or the object of international data transfer with another country other than that where the data was originated, provided that the Country of origin provides a degree of protection of personal data in par with that provided for in the LGPD (art. 4, item IV).

However, if the processing operation is carried out in the national territory and aims at the offer or supply of goods or services or the processing of data from individuals located in the national territory, or even, the personal data object of the treatment has been collected in the Brazil, this must be directly subject to the rules provided for in the LGPD (art. 3).

4 – Price collusion through artificial intelligence softwares

Algorithms are developed from an abstract idea to solve a problem, in other words, they are representations of various methods connected in stages that fulfill a function. In this sense, every time that a solution is created, it becomes the basis for the creation and development of an algorithm. The complexity of algorithms is limited by creativity and can range from the simplest with few variables, information and conditions, to most complex structures and functions. An example of a complex algorithm is the automatic generation of response by natural language processing algorithms. By classifying the meanings assigned to each set of words, sentences can have their meaning classified and their response estimated.

Algorithms that set the prices of products on the Internet work basically through 3 (three) steps. First, the algorithm experiments with different pricing strategies over time. After the search, the algorithm determines which prices are profitable and learns the lessons. Ultimately, the algorithm's choice of pricing strategies changes gradually and relies on those that are most profitable. In other words, it works through simple trial and error, learning as it goes what tends to turn a profit and what does not.[27]

In the long run, there has been a high degree of investment in technology by companies to benefit from an "algorithmic competitive advantage", because if other companies in the sector are using algorithms, the rest end up having a strong incentive to do the same, lest them be left out of the market. The result is a

[27] http://www.frontier-economics.com/uk/en/news-and-articles/articles/article-i2197-algorithms-and-price-collusion/ - Access on 04/18/2020.

certain sector of the market where all competitors use algorithms to constantly monitor the actions of other competitors, consumer choices, and changes in the market environment in real-time and respond to them, thus creating a transparent environment and conducive to a kind of collusion.

However, it can be rather difficult to assess whether algorithms increase or reduce the prospect of collusion, as they tend to modify the structure of the market conditions and supply-side factors, which together could have a positive, negative, or ambiguous impact on the sustainability of collusion.

The problem with algorithms that ultimately allow collusion is that this type of behavior can happen without the developers of the algorithms even knowing, let alone the companies that employ them; that is, the great challenge of a stricter legal measure would be the investigation of how the collusion occurred, whether it occurred as a result of the negligence of the owners of the algorithms to understand what their pricing tools were up to or whether it was just something that the algorithm developed into contact with similar algorithms.

In that sense, there are some traditional measures that antitrust authorities can put in place to address at least some of the competition concerns. These possible alternatives and, in the case, less stringent approaches could include the use of market research, merger control enforcement, and the use of remedies.

Unlike the economic approach, which considers collusion to be a market outcome, the legal approach focuses on the means used by competitors to achieve such a collusive result. Competition law does not generally prohibit collusion as such but prohibits anti-competitive agreements. In that sense, the development of algorithms created solely for the purpose of creating collusion, and thereby achieving higher prices in the market is illegitimate as being an anti-competitive practice.[28]

If the circumstances are sufficiently clear that the algorithm was developed for this purpose, this would not exclude the possibility of excessive pricing based on the established joint dominance. The problem is to prove the existence of joint dominance, since price collusion can be difficult to detect due to the fact that algorithms do not take the form of a unified price that has been maintained for a long time, thus making it difficult to verify whether the price at any given time was really above its competitive level.

The emergence of algorithms and their application in the market has generated concern about the behavioral future of these algorithms inasmuch as there is a possibility that at some point they may help to implement conventional cartel-like behavior. This could be acheived because these algorithms are developed and become capable of processing all available and relevant pricing information and therefore, by monitoring and analyzing or anticipating their competitors' responses to current and future prices,

[28] http://www.oecd.org/daf/competition/Algorithms-and-colllusion-competition-policy-in-the-digital-age.pdf - Access in 04/18/2020.

competitors may be more easily able to find a supra-competitive price balance on which they can agree and maintain it over time and relevant changing circumstances.

A possible countermeasure to the risk of such new types of cartels is the use of other algorithms developed to detect collusive proposals and, in general, possible cartel behavior. Thus, the use of such algorithms will create the possibility of placing the technology at service of antitrust enforcement and competition enforcement.

5 – Ethical limits of personalized prices

Personalized prices and all other tools provided by the use of artificial intelligence, as long as they are used in compliance with the law, represent *a priori* a combination of benefits both to the companies and consumers, as it is a way of facilitating purchase research mechanisms and helping the consumer to have access to products that match his or hers profile. On the other hand, this may prevent them from easily finding all other products they may be interested on, regardless the area of life.

It is important to highlight that here we are addressing the situation where programming process of algorithms shows to the consumer the products whose prices are more compatible to his/her profile, but not the distortion of this technology to change the price of the same product according to the profile of the person, or even the denial to offer a product due to the consumer's profile, known by geo pricing and geo blocking, which, whatever the area of life, amounts to discrimination and other infringements to the Brazilian Consumer Protection Code, for instance, to its articles 4º, caput, items I and III; 6º, items II, III and IV, 37, §2º, and 39, items II, IX and X.

Due to such benefits, it would not be reasonable to prohibit its use in certain areas. However, this should be implemented with a mind to making the use of this technology more compatible with the principles that protect consumers, data subjects and advertising guiding principles, such as transparency, promotional identification and the right to choose to use or not a given technology.

6 – Incorporation of legal requirements and ethical values into the programming process of algorithms to prevent discrimination.

In the same line of the above arguments, there is a need for a specific regulation to guarantee that the programming process of algorithms complies with all objectives and principles of the laws, specially the most recent ones, such as the Brazilian laws no. 12.965/2014 and 13.709/2018, and the recent alterations to the consumer law, that arose exactly from the need to keep up to the technology evolution, in order to prevent discrimination.

Both the GDPR and the LGPD state, quite clearly, that personal data processing activities must be developed - from the beginning - in order to comply with established legal requirements and principles, in order to protect the rights of data subjects, in addition to complying with the fundamental principles that guide Privacy by Design.

The GDPR in its Recital 71 establishes that the treatment agents, specifically the Data Controller, must use appropriate procedures and apply technical organizational measures in order to prevent discriminatory effects against natural persons. And in its Recital 78, it establishes that the personal data processing activities must observe - from its conception - the principles that govern “Privacy by Design”, which, in sum, establishes that any new development of services or products or a new personal data processing activity should always be guided by the search for the defense of individual rights and people's freedom, adapting or creating structured transactions with personal data in accordance with established principles and recognized good practices. In addition, such activities must also comply with the legal requirements listed by the privacy and personal data protection regulations.

Furthermore, Privacy by Design is based on 07 (seven) principles [29], among which are the respect for the user's privacy, always keeping him at the center of the development of activities, products and services.

Like the European Regulation, the LGPD, in its articles 6, items IX and 46, paragraph 2, establishes, respectively, that the activities of processing personal data cannot be carried out with illicit or abusive discriminatory purposes - including in the case of automated decisions - and that security, technical and administrative measures capable of protecting personal data from any form of inappropriate or illicit treatment must be observed from the product or service design phase throughout its execution.

Although the LGPD does not employ “Recitals”, legal requirements and socially and ethically recognized values must be incorporated into the algorithm programming process in Brazil to avoid discrimination.

Brazilian law, as can be seen from Article 20 of the LGPD, quoted many times in this report, also allows the data subject to request the review of decisions taken solely on the basis of automated processing of personal data that affect his interests, including decisions designed to define his profile, be it personal, professional, consumer and credit or aspects of his personality, and the ANPD will be able to carry out an audit to ascertain possible discriminatory aspects in automated processing of personal data.

Of course, this incorporation of legal requirements and ethical values would have to be updated and reevaluated from time to time, given the changing and evolving landscape of consumer and data subject protection.

7 – Human tasks that can be carried out automatically by AI: near future developments.

[29] *Cavoukian, Ann. "7 Foundational Principles". Link:* https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf - Access in April 26, 2020.

It is possible that advertising campaigns, also in the creative field, be able to be carried out autonomously by artificial intelligence.

It is worth mentioning that in 2018 Lexus, the luxury vehicle division of the automaker Toyota, ran an advertising campaign whose script was created by artificial intelligence.

The Artificial Intelligence architecture of Artificial Intelligence Creative Adversarial Network (AICAN) has already been tested in order to generate new artistic works, bearing the minimum requirement of originality, that is, an element capable of differentiating an intellectual work from others previously created by human beings. Through the use of AICAN, the so-called discriminatory neural network has access to a vast database labeled with the various existing artistic styles and then uses such information to identify and differentiate the styles. The neural network called generator does not have access to any existing intellectual work, but generates new images, based on random input data. In addition, the discriminator network emits two distinct signs, which are, by definition, contradictory: the first sign is the classification of “art or not art” and the second sign is “style ambiguity”, that is, how confusing the discriminator network becomes or not in trying to identify the style of the artistic work generated by the generator network, based on the labeled artistic styles. Then, the generator network uses this sign of style ambiguity to improve its ability to generate artistic works that do not follow the existing artistic styles and therefore have an increasing level of style ambiguity. The input data can certainly include advertising campaigns[30].

The project “Generating 'Art' by Learning about Styles and Deviating from Style Norms” carried out by the researcher Ahmed Elgammal from the Art and Artificial Intelligence laboratory at Rutgers University in New Jersey, USA, proposes to maximize the deviation from existing artistic styles and the greatest possible framing of the pre-established art concept, from the point of view of artistic works created by human beings. In Brazil, the protection of intellectual works does not depend on the value or criteria of classification as “art or not art”. In order to assess, especially, the framing of the works generated by AI in the pre-established concept of art, Elgammal conducted experiments, based on the following criteria: whether or not the art was intentional, visually structured, communicative and inspiring. The purpose of this experiment was to compare the response of humans to art generated by the AICAN model in relation to art generated by human artists. The results of the experiment showed that people were unable to make this distinction satisfactorily.[31]

As AICAN is a project developed in the United States, it is believed that the criterion adopted by researchers to measure creativity is different from the criterion used in civil law countries. In Brazil, in general, it is believed that to be endowed with creativity, the work needs to reflect the personality of its creator. Thus, even if a work generated by AI is produced by an AICAN architecture algorithm, it would

[30] FERRO, Vanessa da Silva. *As obras artísticas geradas pela inteligência artificial*: considerações e controvérsias, p. 113. 1a. ed. Rio de Janeiro: Lumen Juris. 2020.

[31] Ibidem, p. 114.

not meet the originality requirement to be subject to protection by the Brazilian Copyright Law. This circumstance does not, however, exclude the possibility of creating an advertising campaign autonomously by the AI. The absence of copyright protection would therefore imply the immediate falling into public domain of such work, except in the event of legislative changes, based on (i) the perception of the work's value and its consequent possibility of appropriation as a legal asset as well as (ii) the justifying theories of Copyright.[32]

Technology has improved several activities in society, increasing productivity among different sectors, besides screenwriting of ad pieces. In this regard, it is possible to highlight the following tasks, which were previously performed only by humans and nowadays are provided or also performed entirely through the application of algorithms – associated or not with artificial intelligence:

(a) Writing of books, articles, papers and further literary material that might be created by algorithms programmed with specific purposes or themes;

(b) The act of searching information (as in links to websites in search engines, content on social media, books in reading apps, songs and audiovisual material in streaming platforms), which does not require a greater effort by humans to find the information since the algorithm already filters and ranks data;

(c) Finding direction and routes, which is an activity usually calculated by GPS and navigation apps, and no longer by a human looking to a map;

(d) Simple communication, once some applications contain algorithms that, combined with artificial intelligence, can simulate entire conversations, without human intervention (for example, Siri and Alexa);

(e) Photoshop and other design adjustments on photos and images online, that no longer requires human intervention;

(f) Driving, considering the existence of automated vehicles that combine artificial intelligence and algorithms.

8 - Personalized election campaigns and democracy

In the digital age, the use of data is essential to enhance the dialogue between candidates and the electorate. However, there is a very narrow link between the correct use of data and its abusive and undue use, which consequently creates a negative impact on the final result of the election campaign processes around the world.

The discussion about fake news and personalized campaigns has increased in the last few years, especially after the specific events with the US presidential election and the BREXIT poll, in 2016. In Brazil, it was not different.

[32] Ibidem, p. 117-160.

With big data, candidates can have access to the preferences and information of each internet user, therefore getting to know which is the best way to attract their attention. Through the use of certain forms of content targeting, such as the dark post, microtargeting, among other strategies, it is possible to shape an artificial scenario close to the one desired by the candidates, depending on how much they are willing to invest in the process.

However, what may seem common and harmless for users/voters, in fact is not.

The use of such strategies, with excessive targeting of content and personalized information can jeopardize the debate between the electorate. Besides promoting alienation and a superficial debate, such strategies can be considered to be manipulative and are, nonetheless, unfair.

In other words, there is a strong and dangerous political polarization, social demobilization and the so-called silencing effect of certain public issues, consequently affecting individual's informational self-determination. Therefore, the undue use of digital strategies to obtain votes during an election shows, in the end, a manipulated result of the campaign, with false data arisen from artificial moves.

The Brazilian authorities started to think about solutions to combat the negative impacts created by electoral strategies, mainly due to the legal omission in regard to those specific tactical maneuvering.

According to Article 5, X and XII of the Brazilian Federal Constitution, the inviolability of intimacy, privacy and honor are fundamental rights, as well as the confidentiality of telegraph correspondence and communications, except in the case of a Court order.

In view of such fundamental constitutional rights, the LGPD establishes that the use of personal data must follow the principles of article 6 of said law, such as the purpose, adequacy, necessity and transparency. With respect to sensitive personal data, which consists on information regarding politics, affiliation and political organization, a special treatment is required by the law - such as, for example, its use linked to the consent provided by the data subject.

In addition to the LGPD, the Electoral Law[33] has been recently adjusted with respect to electoral digital content. Among its changes, the law sets forth that the candidate cannot use false profiles/users to propagate information, especially false information regarding other candidates (creating the so called candidacy deconstruction), under penalty of the payment of a fine.

Despite all the constant efforts of the authorities, the legislation regarding digital strategies on election campaigns is still superficial, while the referred strategies are increasingly accurate, representing a real impact on democracy and a real political polarization without, however, rendering a true portrait of the electorate's will.

[33] Federal Law Nº. 9504/1997