IOSR Journal Of Humanities And Social Science (IOSR-JHSS)
Volume 29, Issue 9, Series 5 (September, 2024) 44-53
e-ISSN: 2279-0837, p-ISSN: 2279-0845.
www.iosrjournals.org

Personal Data Collection In Business As Seen By The Brazillian Data Protection Law (LGPD)

Mateus Ribeiro Lima
(Law Department, Faculdade Baiana De Direito E Gestão, Brazil)

Abstract:
The collection and analysis of large volumes of data -Big Data- in the most diverse formats, from Internet browsing patterns to postings on social networks, allows stakeholders to make better-oriented decisions, solidifying the data-driven business standard. Nowadays, there is an explosion of information, whether through the internet and its social networks, or through corporate applications, as well as cell phones and smartphones, RFID reader tools and video control cameras for traffic, security, etc. culminate in a large mass of highly complex, structured and unstructured data.
Such data are extremely relevant if it is taken into account that they can collaborate to indicate the type of purchase behavior of a certain customer until identifying a crisis in a sector of the economy, migration of consumers to the competition and outbreaks of infectious epidemics, such as the Zika Virus and the H1N1 flu. Turning attention to what is called Big Data is becoming more and more essential, for investing in new technologies, analysis methodologies and adequate software tools. Certainly, we currently have great strength in the information technology scenario, which mobilizes many individuals who research, talk about and seek to understand what it is, how it can be used and how this phenomenon called Big Data is formed.
In this scenario, the debate on the right to privacy and intimacy becomes relevant in the face of the use of this information by companies and organizations, analyzing the vulnerability of the internet user in the face of Big Data and the national and international legislation on the subject, as well as aiming to explore and to describe how companies try to get to know their consumers better, through the analysis of data that are posted on virtual media.
Key Word*: Big Data. Ethics. Information. Privacy. Social media.*

Date of Submission: 05-09-2024 Date of Acceptance: 15-09-2024

I. Introduction

Technological advances in communication have always sought to create a Global Village, enabling the entire world population to have access to a fact simultaneously. This is the principle that guides the creation of global television news networks, such as CNN, in addition to an entire network Broadcast Digital for live broadcasting in real time, from anywhere on the planet.

The financial world also seeks this same ease of communication, investing large sums in modernizing equipment, to enable the creation of a more dynamic financial community. The so-called home-brokers are already a reality (DEMÉTRIO, 2011).

Following the need to reduce expenses and greater controls over branches, companies began to invest more in internal communication networks, connecting all their global operations. In this area, executives fully experience the facilities of fast communication, saving paper, travel, time and telephone calls.

Such contact at work causes a need to expand such benefits to homes. Thus began the movement to install a computer in each home. Convergence goes beyond the economic-corporate treadmill and starts taking technology into the home, interconnecting a network of consumers eager for information, products and services (FARIAS, 2000).

This total convergence promotes new savings for companies, especially in logistics, operational, sales and distribution costs, in addition to implementing a personalized sales channel, with greater effectiveness for its target audience.

Interactivity forces virtual companies to be prepared to serve their consumers anywhere and at any time. In the interactive and virtual world, a company based in Little Rock, Arkansas, lives with the possibility and risk of quickly interacting with a consumer from, say, Mendoza, Argentina, in a reality until little unthinkable time. A person in the interior of Minas Gerais, for example, can buy and sell shares in a company based in Japan and publicly traded on the New York Stock Exchange, USA.

Having an open window to the world requires much more than just the selection of the target audience, it requires the consolidation of legal logistics that reflects the diversity culture of virtual clients/consumers (LEVY, 2018). The internet currently has more than 1.88 billion websites and more than a thousand homepages per day. It refers not only to a virtual community, but to several virtual communities that are formed around common objectives, targeting different tribes with participants from different parts of the planet, from different cultures, each subject to diverse principles, values and norms.

The globalization of society and the economy requires the globalization of legal thought, in order to find instruments for applying norms that can overcome the principle of territoriality, especially with regard to Commercial Law and Criminal Law. This trend of globalization of Law itself is not new. Private International Law somehow already comes, through International Treaties and Conventions, seeking to establish more equitable criteria for legal analysis between the different national States (DEMÉTRIO, 2011). The issue, however, goes far beyond that: new relationship principles must be developed, that is, general guidelines regarding certain basic requirements that should be met by all network users. Solving these issues would already promote greater security in relationships in the virtual world. This is different from creating specific rules whose determination and effectiveness are limited in time and space.

Another reflection arising from the convergent society is the increase in the distance between developed and developing nations, as a result of what is called digital illiteracy, a political-social difficulty consisting of having a mass of workers not prepared to use new technologies. The concern is not only educational: it harms the ability to use labor, even those with higher education (DONEDA, 2006). In the business field, profit is the main objective of every company, however, the way of listening to the customer is also subject to an ethical assessment. Still according to Murgel and Neves (2006), ethics can be used to establish right or wrong actions, which applies, for example, to relationships between companies and their customers. Ethics is situated on a different plane from legislation. This is because a company can act within legal dictates, however, make decisions that contradict ethical values. In this context, it is essential to discuss the security that companies promote regarding said data and the privacy of this data, for example, that contained in social networks, which despite being generated and made available by individuals who, in a certain way, have chosen by making such data public, they certainly did not do so for the purpose of being used by corporations.

The present study is relevant because it seeks to understand and explain the functioning of Big Data and the real protection of Internet users in the involuntary generation of all this content, which motivated us to discuss the issue. In this way, our general objective is to highlight the vulnerability of internet users in the face of the practically involuntary production of information about their habits on the Internet and the consequent commercialization of this content for companies looking to sell products for each specific profile. Therefore, a more in-depth study of the topic is necessary in order to answer the following question: Can the use of Big Data override the right to privacy and intimacy of Internet users?

Through the questions raised, this study seeks to demonstrate that even though it is possible for companies to make use of social media data, they must respect the ethical aspects involved and implement transparent policies for their consumers. To this end, bibliographical research will be used, recognized as a source of secondary data collection, developed from already prepared material, consisting, especially, of books and scientific articles, being relevant for collecting basic information about the direct and indirect aspects linked to the theme under study.

II. Digital Information And Big Data

Nowadays there is an explosion of information, whether through the internet and its social networks, or through corporate applications, as well as through cell phones and smartphones, RFID reader tools and video control cameras for traffic, security, etc., which culminate in a large mass of highly complex, structured and unstructured data.

Until the year 2000, it was possible to say that the world's digital information was around 20%, and there was still a lot of data on paper, books and other documentation. Between 2012 and 2014, the percentage of all information generated that was present in the digital environment rose to approximately 98%. The decline in the costs of computers and data storage systems and the great exponential growth in storage and processing capabilities enabled the dissemination of the use of digital information (MAGALHÃES, 2014).

Such data are extremely relevant if one takes into account how they can help to indicate the type of purchasing behavior of a certain customer until identifying a crisis in a sector of the economy, migration of consumers to competition and outbreaks of infectious epidemics, such as the Zika Virus and the H1N1 flu.

It is worth noting that there is still great difficulty on the part of programmers and analysts to understand and define the difference between data and information, as well as their correlations, which provide what is called information. This difficulty brings as an immediate consequence, problems in understanding, specifying and modeling an application (TAURION, 2013).

The information adds something to the knowledge of the reality under analysis. For example, the dosage of a certain medicine that a patient needs to administer is information that results from the correlation between various disease data and that patient: this is the result of the correlation between evaluated data that form a result. This information may or may not be modeled (recorded) in a structured way and, currently, in unstructured forms, such as posts, comments on social networks, among others.

Data represents records of information. In the past, these were only recorded physically on paper, for example, a medical prescription. Nowadays, with the evolution of systems on mobile platforms for hospitals and doctors, such records are carried out through smartphones, data collectors connected to large hospital networks. It is evident that there are several digital data recording modes, which represents a new application format with great agility. In this way, a series of processes are triggered that influence an observed reality, which can help save a patient's life, by sounding an alarm, for example (TARAPANOFF, 2006).

The processing of information gives rise to different types of data, however, the data must record only the really important aspects of the information, that is, the applications are oriented to the requirements and needs for which they were designed. Therefore, the drug manufacturer's address does not represent a requirement for a control system that maintains the lives of patients during a hospital stay, however, when thinking about the expansion of data and its application, it may currently become relevant for carrying out research into geographic concentrations of manufacturers, or more detailed analysis of locations and climates with regard to logistical aspects for making a medicine available. In other words, there are an infinite number of opportunities to explore any data. They all hold an intrinsic value, or one that has not yet been discovered and analyzed (MEYER; BABER; PFAFFENBERGER, 2015).

Therefore, it can be concluded that in a system of integrated and automated medical monitoring information in networks, in theory, all the information essential to the system's objectives (preserving the patient's life, in the case of the example cited) is contained. But clearly this depends on the requirements when the system is designed. The data from this information will be processed by the designed system. It is known that a computer does not process information, but in reality, data, and the results presented by these systems.

In this environment that becomes faster and more dynamic every day, there is a clear need for these companies to have access to such market changes and for individuals in general, at risk of having their corporate closure.

We are already witnessing the closure and closure of companies that do not prepare themselves for the aforementioned environment of varied information, such as internal business intelligence information to support decision-making, and about their competition, restricting their decision-making actions in the search for improvements because they do not have general information from the digital world, which prevents the taking of survival and competitive maintenance measures (CASTELLS, 2006).

Turning attention to what is known as Big Data becomes increasingly essential in order to invest in new technologies, analysis methodologies and appropriate software instruments. Certainly, we currently have great strength in the IT scene, which mobilizes many individuals who research, talk about it and seek to understand what it is, how it can be used and how this phenomenon called Big Data is formed.

III. The Brazilian Data Protection Law - LGPD

Brazillian Law no. 13.709/2018 (Lei Geral de Proteção de Dados - LGPD), regulates the processing of personal data, including digital media, by natural persons or legal entities governed by private or public law, with the aim of protecting the fundamental rights of privacy and freedom, and the free development of the natural person. The reason that inspired the advent of personal data protection regulations, in a more consistent and consolidated way, from the 90s onwards, is directly linked to the development of the digital economy business model itself, which began to involve a much greater dependence on increase in international database flows, especially those related to citizens, made possible by progress in globalization and technology (PINHEIRO, 2018).

According to Peixoto (2020), with the promulgation of the aforementioned law, some of its legal aspects began to be discussed from the perspective of the Marco Civil da Internet and, in particular, taking into account the Consumer Code (CDC), such as the recent data leak from the company Netshoes in which the MPDFT agreed a Conduct Adjustment Term (TAC) with the company. In this context, it can be said that the performance of companies, in the digital context, carries with it the need to develop instruments for regulating and protecting the personal data of service users, or those who carry out any type of virtual transaction involving the provision of personal data.

Countless actions carried out in virtual space are part of any individual's reality, therefore, the rights guaranteed in the “offline field” must also be guaranteed in the digital environment. Therefore, it is important to point out that national legislation does not only protect personal data in virtual media (PINHEIRO, 2018). It should be noted that European Law (GDPR) is in force, establishing the rules regarding the processing of personal data relating to individuals located in the European Union. It is important to point out that state bodies and Brazilian companies, which maintainlive businesses with European nations, will be obliged to ensure that their data

processing policies are in line with the GDPR, at the risk of penalties, as well as loss of credibility, clientele and brand value in the international market (PEIXOTO, 2020) .

The LGPD has extraterritorial scope, that is, effects at the international level, as it also applies to data that is processed outside Brazilian territory, as long as the collection took place in Brazil, or by offering a service or product to people in Brazil. homeland territory. In this way, personal data processed by a technology company that stores the data outside the country will have to comply with the requirements of the LGPD (PINHEIRO, 2018).

According to Peixoto (2020), the LGPD will have one of the most significant impacts that a Brazilian law has ever achieved. The legal diploma is categorical: all data processed by legal entities governed by private and public law, whose owners are located within the national territory; or its collection took place in Brazil; or even if the objective is to offer services or products in the country, they must follow its dictates. Therefore, it is not an option, but an obligation for companies to follow the personal data protection rules established in the LGPD (PEIXOTO, 2020).

Still according to the aforementioned author, the measures to be taken for protection will be placed in the ranking of social, economic and legal debates in the coming years, as traffic is on the rise and the risks of attacks and data leaks affect practically the entire private and public initiative in a nation. Every day, millions of personal information circulate on virtual networks. Large-scale data exposure is increasingly common, highlighting the vulnerabilities of protocols and systems, even on the part of the State, which should monitor the security of operations (PEIXOTO, 2020).

When collecting data, companies must inform the purpose. The legislation established a series of obligations for them, which must maintain a record of processing activities, so that they can be known, through a request by the holders or analyzed in the event of signs of irregularity by the National Authority. When receiving a request from the holder, the response to the demands must be given within 15 days (VALENTE, 2020).

Businesses will be profoundly impacted, and it is up to institutions and companies to protect themselves from possible penalties and, just as important, demonstrate reliability in the market, ensuring the protection of their databases (PEIXOTO, 2020). Therefore, such entities must adopt measures to guarantee the security of information and notification of the holder, in the event of a security incident. The aforementioned requirement is valid for all agents in the treatment chain.

If a controller causes harm to others, as a result of a processing activity, they may be held responsible and must repair the damage (VALENTE, 2020). There are numerous types of cyber attacks and databases connected to the internet are at a certain level of vulnerability. One of the cases that achieved notoriety of negligence with information was the leak of data from millions of Facebook users to Cambridge Analytica, a British political marketing company.

In Brazilian territory, two recent cases have been confirmed: that of Banco Inter and Netshoes; and another in the investigation phase, that of the credit protection company Boa Vista (PEIXOTO, 2020). In the case of a public entity, the legislation exempts consent in the processing of data for public policies set out in contracts, laws and regulations. AND admitted also the shared use of data by public entities, as long as the principles established in the standard are observed.

In this sense, it is necessary for each body to inform the data processing hypotheses, including the legal basis, purposes and procedures used to do so (VALENTE, 2020). In turn, Peixoto (2020) states that one of the most immediate measures, when exposure and leakage occurs, is to inform the National Data Protection Authority (ANPD) within a reasonable period of time (defined by the authority itself).

The LGPD points out a series of penalties for the event of violation of the established standards, including warnings, with the possibility of imposing corrective measures; fine of up to 2% of revenue, with a ceiling of up to R$50 million; deletion or blocking of personal data linked to the irregularity; partial suspension of database operation; and partial or complete prohibition of the treatment activity (VALENTE, 2020).

Likewise, Peixoto (2020) highlights the relevance of mentioning that there are already companies that work with digital certification for institutional and business websites, as a means of improving credibility, during navigation, by certifying that the website is in line with the LGPD. The Brazillian National Data Protection Authority (Autoridade Nacional de Proteção de Dados - ANPD) is responsible for the inspection process. This body was created with ties to the Presidency of the Republic, with an indication in the legislative text of a study for a more autonomous format.

IV. Sensitive Personal Data: Concept And Distinction

The LGPD introduces the concept of sensitive personal data in inc. II of art. 5th, *in verbis*:

[...] personal data on racial or ethnic origin, religious conviction, political opinion, membership of a trade union or organization of a religious, philosophical or political nature, data regarding health or sexual life, genetic or biometric data, when linked to a natural person (BRASIL, 2018).

The legal technique used in outlining the concepts is initially inappropriate, as the inc. I explains the concept of personal data, while the inc. II of art. 5th of the LGPD does not exactly establish the definition of sensitive personal data, but is restricted to mentioning examples. The aforementioned legislation has a partial classification, distinguishing the data, however, defining only one side of this differentiation, which is why the opposite concepts are stipulated by exclusion.

Thus, based on the definitions of items I and II of art. 5 of the LGPD has the following classification: data: personal and non-personal; and personal data: sensitive personal data and non-sensitive personal data (personal data itself or personal data in the strict sense) (BRASIL, 2018). In this way, initially, data that cannot be included in the definition legal of personal data (art. 5º I), are recognized as non-personal data, not protected by the LGPD. This situation includes, for example, the data of legal entities (which cannot be linked to an individual).

In turn, data related to a natural person that does not fit the legal definition of sensitive personal data (inc. II of article 5) are classified as non-sensitive personal data, or personal data in the strict sense. The LGPD points out, in a merely illustrative list, that sensitive personal data comprises personal data regarding ethnic or racial origin, political opinion, religious conviction, membership of a union or organization of a religious, political or philosophical nature, data concerning life sexual or health data, biometric or genetic data, when related to a natural person.

The matter is controversial and there is no consensus in national doctrine, taking into account that it is also argued that the list is exhaustive, to provide legal certainty to processing agents and prevent doubts regarding which data are recognized as sensitive personal data. However, in theory, it is not possible to defend that the role provided for in art. 5th, II of the LGPD lists all personal data that are recognized as sensitive, nor can it be defined in advance that specific personal data is - or not - sensitive, under any circumstances. In other words, a priori non-sensitive personal data can become sensitive personal data in certain circumstances (BRASIL, 2018).

By way of example, an individual may have a photograph kept in their wallet for months or years, without a specific purpose, and it is personal data (in the strictest sense) capable of identifying its owner. However, when using it to register for a selection process, in a vacancy linked to racial quotas, such photo becomes sensitive personal data. When recognizing the list as being exemplary in nature, there is an absolute legal presumption that such personal data is always sensitive and, in addition to this, other personal data can be classified as sensitive. In this way, there is a deferred protection attributed to the personal data listed in section II of art. 5th of the LGPD, to any genetic or biometric personal data and to others that, perhaps (although not listed in the legislation), fall under the category of sensitive personal data (BRASIL, 2018).

In the field of Comparative Law, art. 4 of the General Data Protection Regulation (GDPR) of the European Union does not include the concept of sensitive personal data, but rather of personal data (art.4.1) and certain personal data that are treated differently, which are biometric, genetic and health-related (art. 4, 13, 14 and 15). Furthermore, art. 9 of the GDPR regulates the "special modalities" of personal data, with the prohibition (rule that includes exceptions) of the processing of personal data that reveal ethnic, racial origin, political opinions, philosophical or religious convictions, or trade union membership, genetic data, biometric data to identify an individual unequivocally, data concerning the health and sexual life or sexual orientation of a subject (CARDOSO, 2018).

The specific legal bases for the processing of sensitive personal data are set out in articles 11 to 13 of the LGPD, which are more limited than those that regulate the processing of personal data that are not sensitive (articles 7 to 10 of the LGPD). Furthermore, there are different rules for processing personal data (sensitive or not) of certain holders, which focuses on children and young people (article 14 of the LGPD), and the processing of personal data carried out by public law legal entities governed by the Access to Information Law (articles 23 to 30 of the LGPD).

Based on these distinctions and the legislative conceptualization, it is necessary to seek greater clarity in the delimitation of data that falls within the classification of sensitive personal data. Taking into account the examples listed in inc. II of art. 5 and the cases of treatments established in art. 11 of the LGPD, sensitive personal data can be recognized as biometric data, genetic data and certain registration or biographical data (depending on their content or the purpose of using the data) which, due to their bias, are protected differently (BRAZIL, 2018).

Biometric or genetic data are explained in a generic way by art. 5th, II of the LGPD, which specifically points out certain genetic data (ethnic or racial origin) and countless biographical data, a large portion of which is linked to freedom of conscience and thought (political opinion, religious conviction, membership of a union or organization of philosophical, religious or political nature) and any biographical and registration data concerning health or sexual life (BRASIL, 2018).

By way of example, the number of a labor case proposed by the holder against his former employer, although registered, represents sensitive personal data and receives differentiated treatment, to avoid possible obstacles to re-entry into the labor market (thus, the art. 4, § 1, II, of CNJ Resolution 121/2010, determines that the names of litigants cannot be used as a criterion for procedural consultation in the labor field) (CNJ, 2010).

In summary, sensitive personal data is data that, due to biometric or genetic characteristics, receives greater protection from the constitutional right to privacy, regardless of the treatment attributed to it and its objective; or concerns peculiarities and information of greater exposure and vulnerability of its holder; or may cause negative discrimination against its holder, taking into account its knowledge and may unduly create obstacles or impediments to access to services, goods or rights. Therefore, the processing options are more limited for personal data of a sensitive nature than for ordinary personal data. Sensitive personal data does not represent a synonym for discriminatory use of data, but only one of the assumptions used in its definition. Therefore, the lack of possibility of discriminatory use of personal data does not mean that said data cannot be recognized as sensitive (CARDOSO, 2021).

By way of example, the LGPD itself establishes, as legal bases for the processing of sensitive personal data, the regular exercise of rights and protection of the physical safety or life of the holder (art. 11, II, "d" and "e") (BRAZIL, 2018). Therefore, they constitute hypotheses in which sensitive personal data are processed by third parties on behalf of their holder. Thus, Regulatory Standard 01 (NR-01) of the Special Secretariat for Social Security and Labor (of the Ministry of Economy) points out, among the obligations of employers, that of providing the Labor Inspection with all information relating to health and safety at work. In this situation, the workers' sensitive personal data is used for a non-discriminatory purpose (and they do not fail to configure sensitive personal data for this reason).

Furthermore, if personal data in the strict sense is used for discriminatory purposes towards its holder, would this be enough to transform it into sensitive personal data? As an example, Law no. 12.414/2011 (Positive Registration Law) regulates the databases developed by financial institutions, containing payment data from individuals or legal entities, with the scope of composing the credit history (BRASIL, 2011). In summary, such databases are made up of registration data (name, ID number, CPF, account and agency number, etc.) and biographical data of the holder (contracts signed, credit amount granted, receipt and payments and the others listed in the art. 4 of Decree no. 9.936/2019 (Regulation of the Positive Registration Law), all falling within the definition of personal data in the strict sense, that is, non-sensitive.

If a financial institution, based on this personal data, denies a property financing request promoted by the holder, as it classifies its score as insufficient for the desired value, would such history of previous debts and credits become sensitive personal data? It is well known that there is no conversion of non-sensitive personal data into sensitive ones (and vice versa) in accordance with their intended use - or not - for discriminatory purposes. This would even allow the same personal data to receive different classifications in different databases, depending on the treatment attributed to it.

Therefore, claiming that sensitive personal data are those directly related to the ability to negatively discriminate against the holder is an incomplete definition and does not correctly separate sensitive data from non-sensitive data. If sensitive personal data is used for a non-discriminatory purpose, it does not become non-sensitive personal data. In the same sense, if non-sensitive personal data is used for a discriminatory purpose, it does not become sensitive personal data.

Personal data regarding ethnic or racial origin, political opinion, religious conviction, membership of a trade union or organization of a philosophical, religious or political nature, data concerning sexual life or health, biometric and genetic data are always classified as data sensitive personal data, even if they are not treated for discriminatory purposes. The aforementioned personal data are recognized as sensitive, as they were selected by the infra-constitutional legislator as deserving greater protection of the right to privacy (regardless of the purpose of the processing); or because they make it possible to access characteristics or information of sensitive vulnerability and greater exposure of their holder, or because they may lead to negative discrimination to the detriment of their holder, taking into account that their knowledge may unduly lead to impediments or obstacles to access to goods, services or rights.

There is no single uniform basis to justify the choice of an exemplary list of sensitive personal data, nor even to identify, in practical terms, whether personal data is sensitive or not. The main difficulty is to assess whether the processing of data may result in negative discriminatory situations, and to what extent they will be sufficient to characterize personal data as sensitive. As a rule, the characterization of data as being of a sensitive nature due to negative discrimination will be verified when the discrimination affects the holder in such a way that he is no longer able to disconnect or separate himself from it. As an example, undue disclosure that an individual has contracted HIV could irreversibly harm them (CARDOSO, 2021).

Therefore, the definition of sensitive personal data encompasses certain characteristics specific to the data, such as biometric (e.g. biometric identification) and genetic (e.g. ethnic or racial origin), and the discriminatory purposes (to the detriment of the holder) that could be pursued through data processing.

V. Misuse Of Data

The high value attributed to data has been followed by concern about obtaining it at any cost, as well as the vulnerability of individuals due to undue treatment, blatant latent or even unwanted consequences.

Manipulation strategies, leaks, cyber attacks, rights violations have been multiplied in the context of data misuse. In this sense, the following can be cited as recent events: household appliances that improperly forward and record conversations of individuals; social media applications that extract personal data from users' friends and family without their authorization; physical activity monitors that post maps of runners' daily routes, including victims of domestic violence and stalking, as well as soldiers on military bases; and dating apps that share their users' HIV status with third parties for commercial purposes (LIMA, 2021).

This shows that the fear that individuals feel about losing control of their data is a reality and not simple speculation. Several data have been lost, used, sold or shared with little or no involvement from the most affected subjects, with a lack of ethical awareness on the part of the responsible bodies.

These practices threaten the security and privacy of citizens. In addition to the personal sphere, they affect democratic and social interests - as seen in the scandal involving the company Cambridge Analytica, posing a risk to the integrity of the companies themselves, market innovation and competition.

Having overcome the understanding of the basic concepts regarding what data comprises, it is necessary to highlight the mistakes in its protection, such as the sale of data and sharing between companies, used as a tactic to reach consumers more, through their purchasing profile, Just as Patrícia Peck Pinheiro highlights, the relevance of data in the virtual field:

[...] the need for a specific law on the protection of personal data arises from the way in which the current business model of the digital society is supported, in which information has become the main currency used by users to have access to certain goods, services or conveniences. (PINHEIRO, 2020, p. 40)

Notably, the sharing of data between business companies and government agencies is prohibited, except when the data holder makes them public, or when the execution of a public activity needs to be shared under the protection of the law, thus exceeding the holder's wishes. When the user chooses not to make their data public, and if there is a violation of consumer rights by companies, such facts become the target of legal demands.

Due to the exponential access to the internet and technological progress, companies extract certain types of information from their consumers, with the name, telephone number, e-mail, address, and image posted on social networks being objects of marketing and use as a means of advertising reach, keeping them in the databases of the companies that collected them.

The main problem is that not only companies have identified the values of the aforementioned data, but also cyber-criminals. This is one of the most harmful cyber crimes of the contemporary period: the motivation for data leaks. Not only small companies commit data breaches, but especially large companies. The confidentiality of personal data must be preserved between companies and consumers, when violated it leads to criminal repercussions.

In this context, the high degree of vulnerability in the technological scenario remains evident, with the protection established resulting from the joint application of the General Data Protection Law and the Consumer Code, in line with the Constitutional Charter, with the purpose of promoting the appropriate sanctions to service providers/suppliers.

VI. The Legal Entity And The Duty To Preserve The Fundamental Rights Of Private Life And Human Dignity

As explained, nowadays, it is no longer possible to remove technology from relationships between consumers and companies which, in the information society, increasingly use personal data to support numerous types of activities, most of them to facilitate everyday actions. Faced with this avalanche of information, which constantly feeds databases around the world, facts emerge that denote the need to regulate the form and destination of this information, which in the context of legal entities, assumes the function of prioritizing the conservation of the integrity of its consumers' data, as one of its responsibilities, given the obligation to fulfill its social function.

The problem that lies between privacy and new technologies is not exclusive to modern times. In 1890, when Warren and Brandeis wrote the seminal paper The Right to Privacy, their main concern was with the new technologies available at the time, such as large newspapers and photographic cameras, which, according to the aforementioned authors, had invaded the sacred environment of private domestic life.

It turns out that in the current society of information and control, this problem has become worse. Technology is increasingly accessible to everyone, given that there are already billions of internet users on the planet, undoubtedly a much larger group than that thought by Brandeis and Warren when dealing with privacy protection (DONEDA, 2006).

In this context, national and international laws repeatedly protect the fundamental right to privacy, for example, art. 5th, .

In this way, concepts of the right to privacy are formed, at least symbolically. In this context, Doneda (2006) highlights that in the current control and information society “the legal system provides people with a set of rights to enable them to make decisions about how they manage their data”. They primarily constitute rights of notice, consent and access regarding the collection, use and dissemination of data. These rights are intended to

provide individuals with control over their personal information. Therefore, through this control, you have the freedom to decide how to balance the costs and benefits of collecting, using and disclosing your information.

Furthermore, the aforementioned author calls this conception privacy self-management, which refers to privacy self-management. According to the aforementioned author, the definition of privacy self-management is based on the individual's consent, seeking neutrality about the substance, that is, whether that specific mode of collection, disclosure or use is good or bad, and focusing on the person's consent through the various private practices.

It seems that the conception of the right to privacy as self-management of privacy, based on individual consent, has been shaping up as the current way of understanding such social manifestation of the context of contemporary information and control. A distinction is also made between information that enjoys greater protection and information that requires less protection, classifying it as sensitive and non-sensitive personal data.

This distinction serves as a criterion for investigating privacy transgressions. The use of sensitive data without the consent of its holder represents a serious offense to privacy, however, the same situation with regard to personal data may not represent an offense, depending on the context in which it is inserted (DONEDA, 2006).

The differentiation in question is yet another way of trying to establish criteria for measuring the violation of privacy in specific cases, since sensitive data requires greater protection than general personal data, which serve solely to identify the subject. However, these also deserve protection and cannot be used in a harmful or arbitrary manner.

In this context, privacy as informational self-management, the collection, use and dissemination of data without the consent of its holder represents a violation of the right to privacy, therefore, an invasion of their private life. It is worth noting that this is a historical idea, constructed to, in a certain way, preserve the subject's autonomy over their own life within a society, since information constitutes an intensely valued asset.

Scandals surrounding privacy violations have been commonplace in recent decades, and in all areas, private and public, social and family. Never before have people been so watched. It is argued that the social benefits of Big Data technologies must be harmonized with the risk that they increasingly present to the privacy of each individual.

The more information collected about each person regarding finances, location, health, electricity use, activities online, among others, concerns arise regarding profiling, tracking, discrimination, exclusion, government surveillance and loss of control.

Perhaps the solution is a deconstruction of the very notion of privacy as self-management, especially regarding the rational capacity for consent, enabling the formation of a more appropriate concept for the protection of individual rights.

Certainly, there are risks related to the use of predictive technologies, because the relegation of decisions about a person's life to automated processes based on algorithms and artificial intelligence raises concerns about discrimination, self-determination and the narrowing of choice. In this context, in a society of control and information, full of massive data systems, it becomes increasingly difficult to ensure privacy, perhaps the subject himself, who has become a commercial product on the internet, based on the following reasoning: when the service is free, the user constitutes the product.

The aggregation of information about individuals with the aim of leveraging this information for other marketing activities has become prevalent in society.

Scholars reaffirm this concern in another way: Big Data technologies benefit organizations and not individuals, since they are considered the product itself, because, if you are not paying for the service, you are not a consumer, but rather the product . In virtual interactions, private information is exchanged for free services. From then on, organizations begin to know all people's preferences, offering products according to their profile.

It is unquestionable that companies must treat their users' data positively, since the inclusion of this information in their databases is part of the beginning of a legal relationship, which can be exchange, purchase and sale, or the provision of services, among others. Taking the infinite possibilities as a basis, what cannot be ignored is the relationship that is established and which needs to be based on the principle of good faith. Allowing such data to be used for malicious purposes, in an illicit or cunning manner, violates the corporate social function in an objective panorama, removing the essentiality of assessing guilt and intent for its characterization. Respecting and safeguarding the privacy of citizens is the role of everyone involved in legal relations, given that, according to Sylvestre (2013), the right to privacy has a “radiation effect” that must be verified by the entire legal order, not limited to the citizen-State relationship, that is, must also be taken into consideration in private relations.

From the perspective of private business law, Diniz (2012) asserts that the entrepreneur must observe the principle of objective good faith (art. 422 CC), to guarantee more equitable conditions in the execution of organized economic activities, and, in this way, taking Based on the theory of the social function of the company, entrepreneurs and business companies must have the power and duty to, in the development of their activities, act in favor of the community, and not exclusively based on their own interests.

It can be said that the development of private law established the need to replace the individualistic business vision with the collective axis, and through the principle of solidarity it became possible to broaden the vision regarding the true scope of business activity. With the entry into force of the Civil Code of 2002, according to the teachings of Cardoso (2010), functionalizing principles were made positive, and the selfish, individualistic and essentially patrimonial bias of the Civil Code of 1916 was exchanged for collectivity, sociality and ethics, exalting itself the value of the human person as a guideline for business activity. Such contours in business activities follow a path that inevitably begins with human beings and their dignity, as objects of all this gear.

Sylvestre (2013) points out that the dignity of the human person manifests the axiological dimension of the regime and democratic institutions, revealing the supreme value where the spirit of the Constitutional Charter dates back. Therefore, there is nothing more relevant in the legal framework that should be protected than human dignity. It represents, still in the opinion of the aforementioned author, the elementary core of fundamental rights, the positive legal source of fundamental rights, the ethical source that ensures unity of meaning, agreement and practical value to the system of fundamental rights. Outlining this new pattern of company-consumer relationships has become a difficult task, which, taking into account the dynamics observed in most legal relationships, is magnified due to the inevitable link with the information society.

In this sense, companies are not prepared to share the wealth created by information with individuals. Crisan, Zbuchea and Moraru (2014) argue that the security of personal data on the internet is no longer possible. All activities of a person online are subject to monetization, taking into account that this person is seen as a product. The authors state that both companies and people themselves should be more responsible with private and sensitive information, given the insecurity online.

Nevertheless, systems of the right to privacy continue to be strengthened. For example, in Europe, Convention 108 and Regulation 12 have the function of eradicating threats to privacy, including those outside the continent, through more explicit data minimization, "right to be forgotten", data portability, " privacy by default", greater extraterritoriality and fines proportional to the size of the business (GREENLEAF, 2014).

According to Greenleaf (2014), attempts like these are routinely unsuccessful, due to the ability of American organizations to acquire, process and use personal data from around the world with few limitations. Privacy standards in other nations don't matter much if personal data can be released to the US "safe harbor." (GREENLEAF, 2014). There is constant tension, territorialization and deterritorialization, freedom and control. The model that currently predominates in the information economy is that of the user-product.

It should be noted that there are places and niches where such a model is not applicable, but this does not make it impossible for it to be the predominant model, on the contrary, on many occasions the exception only confirms the rule. It is worth noting that such a dominant model is not necessarily permanent, however, in order not to be so, it is conditioned either by the bursting of a second internet bubble, or by a joint effort by the rest of the world to reject privacy-invasive commercial practices. It is not impossible or unlikely for this to happen quickly.

VII. Conclusion

Data such as posts on social networks and cookies constitute sources of information available to the Big Data system and can be used by companies so that they can obtain greater knowledge about their consumers, creating promotions according to the profile of each individual. Furthermore, consumers may benefit from receiving offers that best suit their particular needs. However, it is clear that the majority of internet users do not have knowledge about how to use the information available online. From there, the ethical question arises regarding the use of this data, which needs to be discussed more intensively in order to guarantee respect for consumers.

It is essential that individuals have greater control over who can or cannot access their information and are aware of the use that companies are making of this data, however, the subject still lacks legislation that establishes security and identification standards for personal data.

However, even though it is possible for companies to make use of social media data, they must respect the ethical aspects involved and implement transparent policies for their consumers. In the end, with the assessment of the transgressed rights and the implications in the legal environment for those who have their data exposed and improperly used in the face of inappropriate processing of information by companies, it was observed that the damage goes beyond the individual field and affects the collective scope, Bear in mind that such data are not always used in isolation, but to achieve a specific purpose for a specific group of individuals.

For this reason, the company, by promoting the inadequate treatment of this data, fails to fulfill its social function in relation to its consumers/users and, in this way, directly affects its biggest target, which is the search for profit guided by good faith. . And not only that, the company has an obligation to prevent possible leaks of information, as a way of giving credibility to its relationship with the consumer/user.

References

[1]. Bastos, Celso Ribeiro. Comments On The Constitution Of Brazil. Vol. 2, São Paulo: Saraiva, 1989.
[2]. Brazil. Civil Code. Law 10,406, January 2002. São Paulo: Saraiva, 2018.
[3]. _____. Federal Constitution Of The Federative Republic Of Brazil. 1988. São Paulo: Saraiva, 2018.
[4]. _____. Law No. 12,414, Of June 9, 2011. Available At: <Http://Www.Planalto.Gov.Br/Ccivil_03/_Ato2011-2014/2011/Lei/L12414.Htm>. Accessed On: 26 Aug. 2024.
[5]. _____. Law N. 13,709, Of 14 August 2018. Available At: <Http://Www.Planalto.Gov.Br/Ccivil_03/_Ato2015-2018/2018/Lei/L13709.Htm>. Accessed On: 26 Aug. 2024.
[6]. _____. Public Ministry Of The Federal District And Territories. Mpdft Files A Lawsuit Against Banco Inter For Leaking Personal Data. Federal District And Territories, 2018. Available At: <Https://Www.Mpdft.Mp.Br/Portal/Index.Php/Comunicacao-Menu/Sala-De-Imprensa/Noticias/Noticias-2018/10211-Mpdft-Ajuiza-Acao-Contra-O-Banco-Inter-Por-Vazamento-De-Dados-Pessoais>. Accessed On: 26 Aug. 2024.
[7]. Campos, Magna. Manual For Preparing Monographs And Tcc. Mariana: Author's Edition, 2015.
[8]. Cardoso, Oscar Valente. The Protection Of Sensitive Personal Data In Non-Discriminatory Situations. São Paulo: Journal Of Law And New Technologies, 2021.
[9]. Castells, M. The Internet Galaxy: Reflections On The Internet, Business And Society. Lisbon: Calouste Foundation, 2006.
[10]. Cnj. Resolution No. 121 Of 10/05/2010. Available At: <Https://Atos.Cnj.Jus.Br/Atos/Detalhar/Atos-Normativos?Documento=92>. Accessed On: 26 Aug. 2024.
[11]. Demetrio, R. Internet. São Paulo: Cia Das Letras, 2011.
[12]. Diniz, Maria Helena. Annotated Civil Code. 10 Ed, Rev. And Current. São Paulo: Saraiva, 2013.
[13]. Doneda, Danilo. The Protection Of Personal Data As A Fundamental Right. Revista Espaço Jurídica Journal Of Law. Joaçaba/Sc, Vol. 1, No. 2, P. 91-108, Jul/Dec. 2011. Available At: <Http://Editora.Unoesc.Edu.Br/Index.Php/Espacojuridico/Article/View/1315/658>.Accessed On: 26 Aug. 2024.
[14]. Doneda, Danilo. From Privacy To Personal Data Protection. Rio De Janeiro: Renew, 2006.
[15]. Farias, Edilsom Pereira De. Collision Of Rights - Honor, Intimacy And Private Life And Image Versus Freedom Of Expression And Information. 2nd Ed. Porto Alegre: Current, 2000.
[16]. Gil, Antônio Carlos. Social Research Methods And Techniques. 5 Ed. São Paulo: Atlas, 1999.
[17]. Greco Filho, Vicente. Telephone Interception. Considerations On Law No. 9,296 Of July 24, 1996. 2nd Ed. São Paulo: Saraiva. 2005.
[18]. Levy, P. Collective Intelligence. São Paulo: Loyola, 2018.
[19]. Lima, Daniela Cenci. The Value Of Data: Brief Considerations On Monetization, Control And Protection. São Paulo: Journal Of Law And New Technologies, 2021.
[20]. Magalhães V.R.V. Et Al. The Use Of Big Data In Violating Users' Privacy For Business Strategies.Canindé: Ifce, 2014.
[21]. Mendes, Laura Schertel. Privacy, Data Protection And Consumer Protection: General Guidelines Of A New Fundamental Right. São Paulo: Saraiva, 2014.
[22]. Meyer, M.; Baber, R.Pfaffenberger, B. Our Future Is The Computer. São Paulo: Bookman, 2015.
[23]. Murgel, D; Silva, J; Neves, J. Business Ethics As A Competitive Differentiator. São Paulo: Enegep, 2006.
[24]. Peixoto, Andrea Stefani. Data Protection Law: Understand In 13 Points!. 2020. Available At: <Https://Www.Politize.Com.Br/Lei-De-Protecao-De-Dados/>. Accessed On: 26 Aug. 2024.
[25]. Pinheiro, Patrícia Peck. Protection Of Personal Data: Comments On Law No. 13,709/2018 (Lgpd). São Paulo: Saraiva Educação, 2018.
[26]. Pinheiro, Patrícia Peck. Protection Of Personal Data: Commentary On Law 13,709/2018 (Lgpd) – 2nd Ed. – São Paulo: Saraiva Educação, 2020. Available At: <Https://Integrada.Minhabiblioteca.Com.Br/#/Books/9788553613625/>. Accessed On: 26 Aug. 2024.
[27]. Prado, Geraldo. Limit Telephone Interceptions And The Jurisprudence Of The Superior Court Of Justice. 2nd Ed. Rio De Janeiro: Lumen Juris, 2012.
[28]. Saconni, Luiz Antônio. Mini Dictionary Bags From Portuguese Language. São Paulo: Current, 1996.
[29]. Sampaio, José Adércio Leite. Right To Intimacy And Private Life: A Legal Vision Of Sexuality, Family, Communication And Personal Information, Life And Death. Belo Horizonte: Del Rey. 2012.
[30]. Sylvestre, Fábio Zech. The Fundamental Right To Privacy In The Face Of Public Administration. Ii International Law Symposium: Material And Effective Dimensions Of Fundamental Rights. 2009.
[31]. Tarapanoff, Kira. Intelligence, Information And Knowledge In Corporations. Brasília: Ibict And Unesco, 2006.
[32]. Taurion, C. Big Data. Rio De Janeiro: Brasport, 2013.
[33]. Valent, Jonas. Understand What Changes With The General Data Protection Law. 2020. Available At: <Https://Agenciabrasil.Ebc.Com.Br/Geral/Noticia/2020-09/Entenda-O-Que-Muda-Com-A-Lei-Geral-De-Protecao-De-Dados>. Accessed On: 26 Aug. 2024.