v. 3, n. 9, 2023

Scientific Journal of Applied Social and Clinical Science

A STUDY ON THE PERCEPTION OF SECURITY THAT DIGITAL LAWS EXERCISE ON USERS OF DIGITAL SERVICES AND PRODUCTS

Nathan Novais Borges
(IC)

Fabio Silva Lopes
(Advisor)
Support: PIBIC Mackenzie

Abstract: Laws that cover the digital context in relation to data protection are becoming increasingly common, such as the Brazilian LGPD (General Data Protection Law) and the GDPR (General Data Protection Regulation). The creation of data manipulation and collection regulations, which cover the digital context, are a consequence of the growing expansion of the digital world along with the exponential increase in data production. The main objective of such legislation is to regulate the storage, processing and use of personal data, with the aim of protecting and guaranteeing the security of data subjects. However, many individuals have deficiencies in terms of knowledge of laws that cover the digital context and good practices on behavior and experience within the virtual world, creating security vulnerabilities for such people. Among the main factors that accelerated the adoption of computing services by people with less familiarity with technology, we can mention the international pandemic of covid-19, which, by creating a scenario of change in society's behavior aimed at greater social distancing, generated both a increase in interactions through digital media and an escalation in the number of digital scams. Based on this scenario, this study seeks to understand how individuals, increasingly associated with a digital context, understand and understand the digital laws created to protect them.
Keywords: Data Regulation Laws, Data Security, Digital Citizen

INTRODUCTION

Federal Law number: 13709, of August 14, 2018, better known as LGPD (General Data Protection Law) (Brazil, 2018), came into force in September 2020, inspired by international legislation, such as the European GDPR, which are becoming increasingly common on the world stage.

The Law in its Article 1:

> "...provides for the processing of personal data, including in digital media, by a natural person or by a public or private legal entity, with the aim of protecting the fundamental rights of freedom and privacy and the free development of the personality of the natural person" (Brazil, 2018).

Therefore, the Law was created to regulate the treatment and collection of data, which are produced in abundance every day by different types of users, offering greater digital security for people. Taking into account the exponential growth in data production, reinforced by the acceleration of digitalization in the world since 2020, the LGPD proved to be a watershed in the Brazilian digital context.

In addition, the international COVID-19 pandemic vehemently accelerated the digitization of various processes, both for users already accustomed to the daily use of technology and for those who had little or no familiarity with digital tools and processes.

By relating the significant evolution of data extraction and analysis capacity, together with a growth in the number of users who are unfamiliar with the computational context, a fragile scenario is created for the security and privacy of the user, who often does not understand their rights guaranteed by the Law covering the digital world. This way, it becomes important to understand the security risks within the digital environment that such a situation can provide to the user, and what is their level of understanding towards their rights and responsibilities according to the established Law.

Therefore, the objective of this study will be to better understand people's perception of the LGPD, considering the impacts on society in a context of growing digital insertion.

Thus, this work was structured as follows: Theoretical Framework, with the objective of carrying out a bibliographic review and a study with studies and concepts that contemplate

this study.

Methodology, in which the methods and approaches adopted in this study are detailed; Results and Discussion, in which the data and results acquired from the scope defined within the methodology are presented, and an analysis of the information acquired along with the knowledge acquired from the Theoretical Framework is carried out; Final considerations, in which the main topics are resumed together with a conclusion of the study carried out.

THEORETICAL REFERENCE

HISTORY OF DATA PROTECTION LAWS

BILL OF RIGHTS OF RIGHTS – 1948

The regulation and protection of personal information is an issue that has been debated for a long time. However, from the Universal Declaration of Human Rights, created by the UN in 1948, the subject became more relevant.

Article XII provides for the protection of the right to privacy "No one shall be subjected to interference with his private life, family, home or correspondence, nor to attacks on his honor and reputation. Every human being has the right to the protection of the law against such interference or attacks."

In 1950, the European Convention on Human Rights sought to reaffirm the protection of the same right in its Article 8. However, even though it is a significant advance in relation to the right to privacy, it is important to realize that at this initial moment, Article 8 states that this right could be violated by a public authority, according to the situations listed. Furthermore, it is not clear how and by whom this protection of privacy must occur and be guaranteed.

DIRECTIVE: 95/46/CE – 1995

The 1995 European Directive is another milestone in the history of data protection regulation. Launched at a time when the internet and the digitalization of services were beginning to consolidate more and more, the Directive was created to be used within the member countries of the European Union (EU), and could also serve as an example for non-members.

It aimed to regulate the collection, formatting, use of personal data, and here personal data can be defined as "any information relating to an identified or identifiable natural person", being "considered identifiable anyone who can be identified, directly or indirectly, namely by reference to an identification number or to one or more specific elements of their physical, physiological, psychological, economic, cultural or social identity".

Another important definition that the Directive brings is that of sensitive personal data, defined as "personal data that reveal racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, as well as the processing of data relating to health and sex life".

Directive 95/46/EC proved to be of severe importance for the time it was adopted, defining not only the regulation of data within the European Union itself. It established the need that companies operating in European territory must guarantee the protection of personal data when sending personal data outside the European Union, otherwise, they could be violating the Directive and create legal problems.

GDPR (GENERAL DATA PROTECTION REGULATION) – 2016

Directive 95/46/EC, which was in force since 1995, was not able to keep up with the growing pace of expansion of the digital world along with the growth in data production. In this context, a review of the Directive began to be discussed.

In 2016, the European Union approved the GDPR, General Data Protection Regulation, which represented a milestone in terms of regulations on the use of personal data. The Law aims to regulate the storage, processing and use of personal data in the European Union.

The Directive, used as the basis for the creation of the new European data regulation, was in force until May 24, 2018, being replaced by the GDPR on May 25, 2018. Unlike the Directive, the GDPR is a Regulation and must be adopted in all EU members.

Compared to the previous Directive, the GDPR presented significant changes, bringing the introduction of new individual rights, such as: the right of oblivion, in which the holder's data stored by an organization must be erased in case of the holder's request; the right to portability, which guarantees the holder's right to demand the transfer of their data from one company to another; the introduction of mandatory notification in cases of data leaks; the need for a data protection officer; the application of fines and penalties in cases of violation of the Law.

This way, the GDPR, which aims to guarantee the security of personal data by regulating how such data can be manipulated and collected by companies, is serving as a reference for the creation of other legislation regarding data protection, such as the LGPD in the Brazilian context.

LGPD (GENERAL DATA PROTECTION LAW) - 2018

Until then, Brazilian legislation provided for the protection of personal data in some internal rules. It is possible to quote:

(i) 1988 - Federal Brazilian Constitution - article 5 - § 10: "the intimacy, private life, honor and image of people are inviolable, ensuring the right to compensation for material or moral damage resulting from their violation", that is, the private life of the natural person is protected by the Constitution, subject to compensation if violated";

(ii) 1990 - Consumer Protection Code - article 43 - "The consumer, without prejudice to the provisions of article 86, will have access to existing information in records, files, records and personal and consumer data filed about him, as well as about their respective sources.";

(iii) 2014 Marco Civil da Internet – Seeks to establish guarantees, principles and duties in relation to the use of the internet in Brazil.

However, such norms did not establish a clear and objective regulation in relation to the manipulation and protection of personal data, a necessary factor in a growing condition of production of information through data. Patricia Peck, in her book "Personal data protection: comments on Law number: 13,709/2018, elaborates:

> "The LGPD was created with the aim of protecting fundamental rights such as privacy, intimacy, honor, image rights and dignity. It can also be pointed out that the need for specific laws for the protection of personal data has increased with the rapid development and expansion of technology in the world, as a result of the developments of globalization, which brought as one of its consequences the increase in the importance of information. This means that information has become a highly relevant asset for government officials and businessmen: whoever has access to data has access to power."

In this context, the LGPD (General Data Protection Law) was approved in August 2018, taking effect from August 2020, seeking to bring a national scenario with greater digital security.

The Brazilian law in its article 5 provides important definitions of terms and concepts.

The following are some terms defined by the Law, which are widely covered in this study:

(i) personal data - information related to an identified or identifiable natural person;

(ii) sensitive personal data - personal data about racial or ethnic origin, religious conviction, political opinion, union affiliation or religious, philosophical or political organization, data referring to health or sex life, genetic or biometric data, when linked to a natural person;

(iii) consent - free, informed and unequivocal statement by which the holder agrees with the processing of his personal data for a specific purpose;

The adoption of the LGPD is foreseen for any case of data manipulation that occurs in Brazilian territory, that is, even if the processing operation is carried out outside the national territory, if the data were collected in Brazil, the application of the Law is valid. The application of the GDPR is carried out in a similar way at the European level, meaning that data collected within the European Union must be handled in accordance with European law.

Another essential factor to be understood is the consent of the data subject. The Law provides for specific and prominent consent, understanding that the holder is the one who can allow the collection and manipulation of their data.

Data processing must comply with requirements established by law. According to Patricia Peck (2018) "The LGPD highlights that the processing of personal data must observe good faith and have a purpose, limits, accountability, guarantee security through security techniques and measures, as well as transparency and possibility of consulting the holders. In this topic, it is possible to analyze a notable difference between European and Brazilian legislation. The GDPR, compared to the LGPD, elaborates in a more detailed and clear way the requirements to be followed for the processing of personal data.

Several companies have sought to adapt to comply with the LGPD standards, and this way, seek to understand the Law. However, the common citizen often does not understand the digital rights that the Law guarantees. A problem that exists in the digital culture of users, which in itself is very limited, to the point of not understanding their own rights and responsibilities in an online world that is increasingly present.

INCREASE IN INTERNET USAGE

The LGPD was not the only important factor in the digital experience in 2020. The international COVID-19 pandemic, which Brazil has been facing since March 2020, was one of the factors that most influenced a greater digital experience by the entire population.

According to the survey carried out by ABComm (Brazilian Association of Electronic Commerce) with the Buy & Trust Movement, revenue grew by around 56.8% in the first 8 months of 2020, as well as the number of digital transactions that grew by around 65.7%. Therefore, it can be seen that several processes have been digitized, in addition to that many people, who were not familiar with digital tools, found themselves in a situation of quickly learning how to behave in a digital world, an experience that in most cases is delicate.

The situation described above was observed by Cetic.br research, which identified a relevant increase in the number of online purchases by classes C, with an increase from 37% to 64%, and in classes D and E with an increase from 18% to 44%. That is, people with less education and less familiarity with the online world, in a short period of time,

began to migrate to a digital environment.

Moreover, in a condition in which the use of the internet is increasing by users, there is a concomitant increase in the production of data and new ways of extracting value and relationships from them. In this scenario, it is able to observe the phenomenon known as Big Data, characterized by the high processing speed, volume and variety of data and information stored in databases, which can be defined as "[...] the capacity of a society to to obtain information in new ways in order to generate useful ideas and goods and services of significant value. Thus, the real revolution is not in the machines that calculate data, but in the data itself and the way we use it" (MAYER-SCHÖN-BERGER; CUKIER, 2013).

By relating the rapid evolution of data extraction, processing and analysis technology to the lack of transparency regarding the way such data is treated and manipulated, potentially harmful situations are created for those who provide their personal data, thus "[...] the combination of apparently harmless data from different databases or the analysis of large databases can generate potentially dangerous information for individuals, organizations and even states, and this is difficult to predict with sufficient anticipation"(Breternitz, Vivaldo & Lopes, Fabio & Silva, Leandro, 2013).

The article "Malice Domestic: The Cambridge Analytica Dystopia", written by Hal Berghel, addresses the scandal of Cambridge Analytica, which was accused of interfering in the 2016 presidential elections in the USA, by using the bad practice of sharing data practiced by Facebook.

User-generated data shared by Facebook and other sources was used to profile voters and target pro-Trump advertisements and materials and messages against candidate Hillary Clinton. Among the data used for this strategy were names, professions, contacts, place of residence, frequented places, and habits. Such data was collected without the knowledge of the users and later used to influence the voters themselves.

It is possible to draw a parallel between the passage described above and the article "What is data justice? The case for connecting digital rights and freedoms globally", by author Linnet Taylor.

In this article, the idea of "data rights" is addressed, which determines ethical paths to be taken in a world of data.

According to the author, the manipulation and monitoring of people becomes more and more assertive, since the connections between databases become more and more accurate. Such characteristics tend to infringe the population's privacy rights and open the discussion about how correct it is to use such data, often generated without public consent.

Thus, a framework of fragility is created with regard to the digital security of users, by relating factors such as the expansion of the digital environment in everyday life, the need to adopt digital tools, added to the rapid evolution of technology, in contrast to a more slow and gradual user perception of the risks related to the availability of their data.

SURVEILLANCE WITH DATA

The growing interaction between people and the digital environment was due to several factors, including the COVID-19 pandemic. The change in society's behavior towards greater social distancing has generated an increase in interactions through digital media. With the increasing use and dependence on Information Technology services, it was possible to observe an increase in cyber attacks.

In a report called Fraud & Abuse Report, carried out by the American company Arkose Labs, which specializes in the area of information security, Brazil was among the

top 5 countries with the most virtual fraud. There has been a huge increase in fraud in e-commerce, the online gaming industry and attacks against devices used to work remotely. That is, all sectors that received a greater flow of data during the pandemic period, suffered more virtual blows.

A great example of digital fraud occurred at the beginning of 2021, a mega data leak that affected more than 200 million Brazilians, which generated insecurity and distrust on the part of the population for not knowing what was leaked or who has access to such data. data clearly. Among such data, CPFs, names, dates of birth, vehicle information, CNPJs, among others, were leaked. Such a leak makes several individuals vulnerable to the most diverse digital crimes.

According to Gordon and Ford (2006), digital crimes can be separated into two categories, one focusing on the technical issue and the other focusing on the human factor.

The first has a more technical nature, and can be characterized by hardware or software failures, and often become vulnerable to hacker attacks. In this circumstance, the solution is given through the same technology, focusing on security issues, from planning to implementation, aiming at safer software and hardware.

An example of technical failure could be seen right at the beginning of the pandemic. In a context of social isolation, virtual meeting platforms have achieved great adherence by people looking for new forms of communication.

Among these platforms, the Zoom application was highlighted for demonstrating digital security flaws. In his text "PANDEMIC IN THE PANDEMIC: THE SCALE OF CYBER ATTACKS POST COVID-19" (2020), Nagli discusses: "In a context of social isolation, virtual meeting platforms have achieved great adherence by people looking for new forms of communication. Among these platforms, the Zoom application was highlighted in the mainstream media for demonstrating digital security flaws.".

The second category, related to the human factor in the interaction between person and machine, occurs in several cases where the user, due to lack of knowledge about the correct procedures within the digital environment, creates security gaps. According to Verizon's "2021 Data Breach Investigations Report" (DBIR), about 85% of data breaches involved human interactions, making clear the relevance of the human factor in data security. The solution in this case is via educating the individual in relation to how to interact with the digital environment.

When discussing people's behavior in the digital world, the term digital citizen becomes important for the discussion. According to Mike Ribble, 2011, a digital citizen can be defined as someone who uses technology effectively and appropriately.

Digital citizenship has another definition, according to Searson, Hancock, Soheil, & Shepherd, 2015, digital citizenship can be defined as the set of qualities required for citizens to use digital tools in various digital environments in an appropriate manner. In his 2015 book "Digital Citizenship in Schools: Nine Elements All Students Must Know", Ribble lists the nine elements that make up digital citizenship. Among these factors is Digital Security, defined by the author himself as electronic precautions to ensure security. This factor is often ignored, by not reading terms of contracts on websites and applications, not taking due care with personal security passwords. These situations are curious, since in the physical world the behavior tends to be the opposite, we put locks and locks on doors, install security devices at home, surveillance cameras, etc.

Together with digital citizenship, there is

the term digital literacy, which according to Martin, can be defined as:

> "the knowledge, attitude and ability of individuals to appropriately use digital tools to identify, access, manage, integrate, evaluate, analyze and synthesize digital resources, building new knowledge… enabling constructive social actions, and reflection throughout this process" (Martin,2006, p.155).

Such concepts as digital citizenship and digital literacy are directly related to the individual's education regarding security in the digital world. Thus, within an increasingly digital context, a scenario considerably accelerated by the pandemic as discussed above, the issue of security is not isolated from the rest of users' digital experience. In addition, understanding the Law, which covers the digital context, will also be a fundamental part to be understood by all, since drawing the fine line between the physical and virtual world becomes progressively more difficult.

METHODOLOGY

From the scenario presented throughout the theoretical framework, and considering the lack of studies related to the level of perception of individuals towards digital laws, an exploratory study was carried out, which according to Gil (2012, p. 12), " their main purpose is to develop, clarify and modify concepts and ideas, with a view to formulating more precise problems or researchable hypotheses for further studies". This way, bibliographical researches related to the theme of Digital Laws and themes related to their context were carried out, aiming to understand the technical level of information available that would help answer the question "What is the level of people's perception in relation to the rights and responsibilities that the Does the General Data Protection Law impose?".

The choice of methodology to be used was quantitative. The quantitative methodology, according to Lozada and Nunes, "uses structured data collection instruments, such as questionnaires, to capture data, which are generalized from a sample to the entire studied population". The exploratory study through the review of the bibliography, helped in the conception of the questions present inside the research form.

In order to understand the characteristics and behaviors of individuals within the digital environment that is involved by the LGPD, a search form was created using the Google Forms tool, an application created by Google to create and submit online forms, which was available for reception of responses over 29 days, from June 30, 2022 to July 29, 2022.

With the information obtained from the form, a quantitative analysis of the data will be carried out through the construction and comparison of graphs, seeking to understand and describe the relationship between the user's behavior within the digital environment and their understanding of the Law.

Thus, the questions were divided into two sections: preliminary and behavioral.

The respondent qualification section aims to classify respondents based on their education, age, location and internet consumption, seeking to understand the profile of the participants.

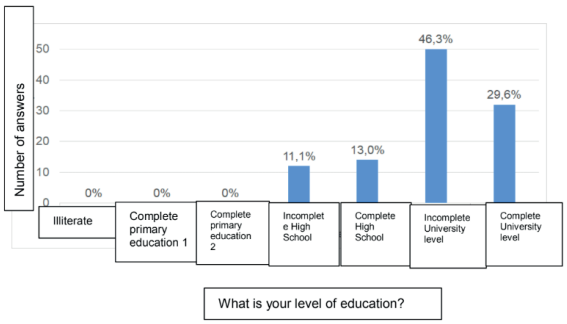
The behavioral section has questions aimed at understanding the level of perception of respondents in relation to Digital Laws. To compose part of the questions inserted in the behavioral section of the form and measure subjective values, such as perception, this study used the Likert scale, which "consists of taking a construct and developing a set of statements related to its definition, for which the respondents will issue their degree of agreement." (Júnior, Severino Domingos da Silva, and Francisco José Costa). (2014).

The results of this study will be subject to the limitation of the responses provided by the surveyed population. Thus, the generalization of the data obtained from the form does not guarantee that the results are the same in any place, period or other group, other than the group of participants analyzed within this study.

RESULTS AND DISCUSSIONS

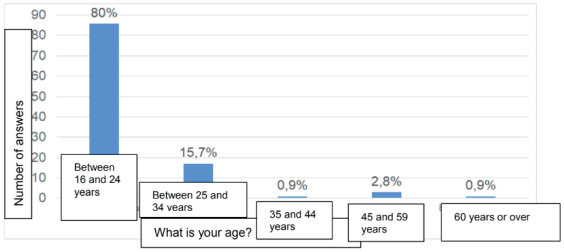
With a total of 108 responses collected over 29 days, the "Perception of Digital Laws" questionnaire delivered a clipping of how people of different age groups and levels of education interact on the internet, along with how they understand the risks, benefits, and security of the availability of your data.

Considering all the responses, 11.1% of the participants claimed to have completed High School, 13% said to have completed High School, another 46.3% reported to have completed Higher Education and 29.6% said to have completed Higher Education.



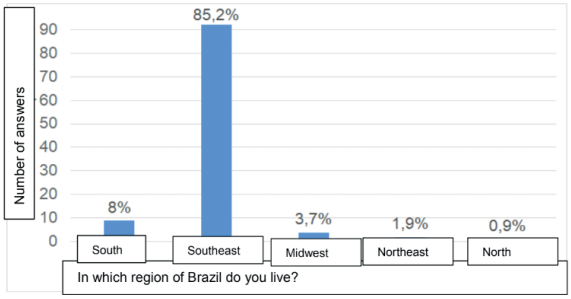
Search Quality Information COVID19 – Question: What is your level of education? [Figure 1]

Of the 108 responses collected, 79.6% of the participants said they were between 16 and 24 years old, 15.7% said they were between 25 and 34 years old, 0.9% reported being between 35 and 44 years old, and 2.8% between 45 and 59 years old and another 0.9% reported being 60 years old or older. Thus, 95.3% of the people involved in this research are between 16 and 34 years old.



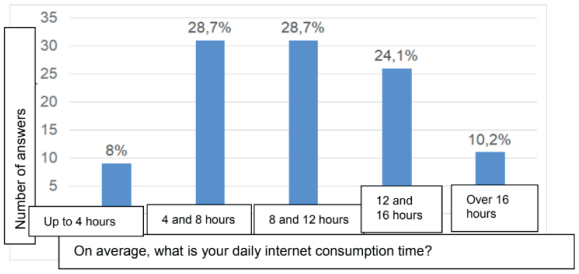
Search Quality Information COVID19 – Question: What is your age group? [Figure 2]

Those who participated in the study also informed the region in which they live, and according to the results obtained, most of the participants, represented by 85.2%, claimed to live in the Southeast, while 8.3%, 3.7%, 1.9% and 0.9% said they lived in the South, Midwest, Northeast and North, respectively.



Results: Search Quality Information COVID19 – Question: In which region of Brazil do you live? [Figure 3]

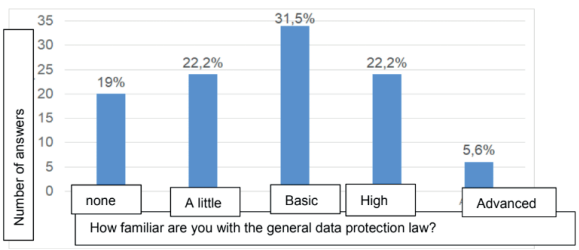
Seeking to understand the level of daily interaction of the participants with the internet, the questionnaire asked people what the average daily internet consumption time was for each person. Regarding this issue, 8.3% of participants reported having an average time of up to 4 hours. The number of participants who claimed to have between 4 and 8 hours or 8 and 12 hours of daily internet consumption was the same, both 28.7%. Part represented by 24.4% of the participants said they use the internet between 12 and 16 hours, while 10.2% answered to use more than 16 hours.



Research Quality Information COVID19 – Question: On average, what is your daily internet consumption time? [Figure 4]

After answering the preliminary questions, used to create a socio-demographic profile, the participants began to answer questions in the behavioral section, with the aim of understanding the level of perception of respondents in relation to Digital Laws.

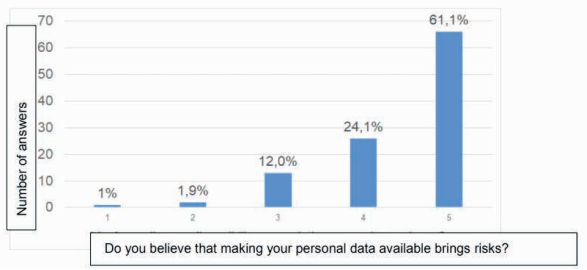
The first question in this section was about how familiar people are with the LGPD. Among all participants, 18.5% said they had no knowledge or familiarity with LGPD, 22.2% said they had little familiarity, 31.5% answered basic, another 22.5% considered their familiarity to be high and 5.6% said to have an advanced degree of familiarity. Among those who responded to have a high level of familiarity with the LGPD, the largest portion is represented by those who use the internet from 12 to 16 hours, with a total of 33%.



Search Quality Information COVID19 – Question: How familiar are you with the LGPD (General Data Protection Law)? [Figure 5]

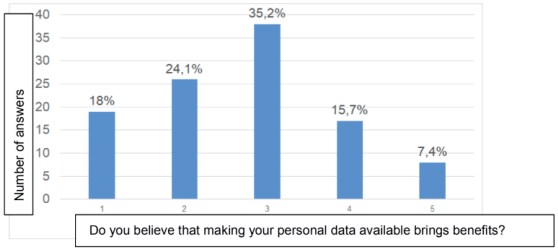
After understanding the degree of familiarity with the LGPD, the participants answered questions related to the availability of their personal data, a central topic of the General Data Protection Law, with the aim of understanding people's perception of risks, benefits and trust. in making such data available. These questions adopted a gradual scale from 1 to 5, with 1 being completely disagree and 5 being completely agree.

The participants answered the question "Do you believe that making your personal data available brings risks?". Based on this question, it was possible to observe that most respondents believe that making their data available brings risks, with 85.2% who answered 4 or 5, in contrast to 2.7% who answered 1 or 2.



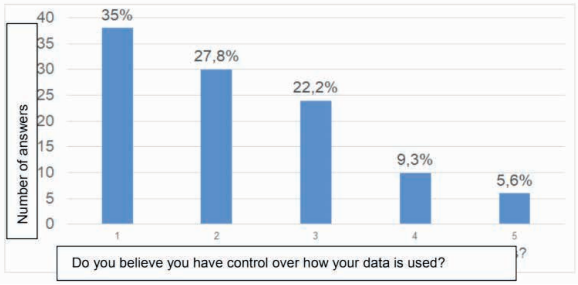
Search Quality Information COVID19 – Question: Do you believe that making your personal data available brings risks? [Figure 6]

Participants were also asked the question "Do you believe that providing your personal data brings benefits?". In this question the results were more balanced in relation to the question of risks, 41.7% answered 1 or 2, while 23.1% marked 4 or 5 and a total of 35.2% selected 3 as an answer. Despite a greater balance in relation to the previous question, there was a greater tendency of responses contrary to the statement that providing personal data brings benefits.



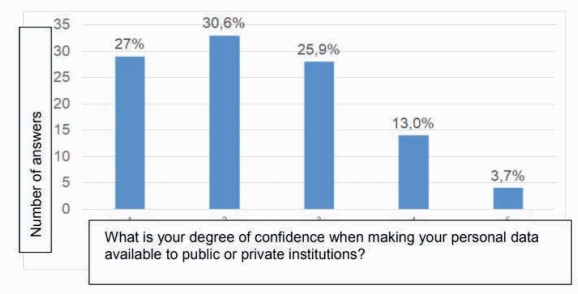
Search Quality Information COVID19 – Question: Do you believe that providing your personal data brings benefits? [Figure 7]

In order to understand the perception of respondents regarding the control of their data, the question "Do you believe you have control over how your data is used?" was asked. Participants demonstrated greater disagreement with the question, with 63% of people answering 1 or 2, in contrast to 11.9% who marked 4 or 5. Among the participants who said they had a "basic" level of knowledge about to the LGPD, 70.6% said 1 or 2, a higher number compared to the total number of responses.



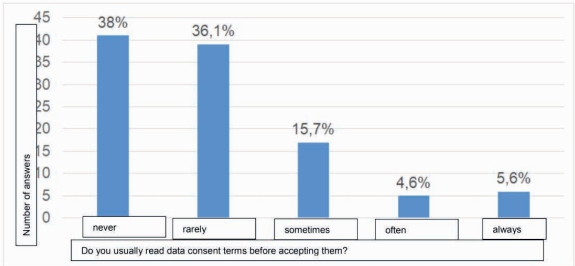
Research Quality Information COVID19 – Question: Do you believe you have control over how your data is used? [Figure 8]

Respondents also answered the question "What is your degree of confidence in making your personal data available to public or private institutions?". The answers to this item showed a tendency similar to the previous question related to the control of their personal data, and in this question the participants also showed a tendency towards a lower degree of confidence when making their data available. 57.5% of respondents answered 1 or 2, as opposed to 16.7% who answered 4 or 5. Among participants who said they had a "basic" level of knowledge regarding the LGPD, 64.7% stated 1 or 2, a higher number compared to the total number of responses.



Search Quality Information COVID19 – Question: How confident are you when making your personal data available to public or private institutions? [Figure 9]

In order to understand how the participants behave in a situation where personal data is made available, the question "Do you usually read the data consent terms before accepting them?" was asked. Among the 108 interviewees, 38% of the participants said they never read the data consent terms, 36.1% said they rarely read them, 15.7% reported that they eventually read them, while 4.6% and 5.6% indicated often and always, respectively.



Research Quality Information COVID19 – Question: Do you usually read data consent terms before accepting them? [Figure 10]

Therefore, throughout the analysis of results, it is possible to note that the majority of respondents tend to believe that there are risks when making their personal data available, along with a lack of control over such data.

However, even in the face of this pessimistic scenario in relation to the availability of data, they are not in the habit of reading the data consent terms before accepting them, demonstrating a contradiction, since not reading such terms decreases the individual's knowledge about what data will be made available and how it will be treated.

FINAL CONSIDERATIONS

This article sought to enable a greater understanding of the level of understanding and perception of people in relation to the LGPD. Within a context of greater use of the internet and digital services, greater data production and an increase in the number of virtual frauds, factors driven by the COVID-19 pandemic, legislation related to data regulation, such as the LGPD and the GDPR become increasingly necessary, in order to protect the personal data of data subjects.

In a context of technology expansion, concomitantly there is an evolution in data collection, treatment and analysis processes, generating new ways of extracting patterns and information. This fact makes it possible to create potentially harmful situations for data subjects, since data association can generate information that violates users' right to privacy, who often do not understand what data is being made available and how it will be used.

The evolution of technology, together with greater digitalization of processes, has brought changes to the daily lives of many people, changing the way they interact and consume services. However, a considerable portion of the public that had their digital experience stimulated does not have the knowledge or skills to interact within the digital world in an appropriate and safe way. This way, it is possible to observe a rapid evolution of technology, greater adoption of digital tools, in contrast to a curve of slower and more gradual development of the user towards their education within the digital context, providing a framework of fragility for their data security.

Thus, concepts such as digital literacy and digital citizenship fit into this scenario of individual education, which within the digital context must understand their rights and responsibilities within the virtual world, being able to use digital resources and tools appropriately and constructive. This way, understanding and having an understanding of the Law that aims to protect the user's data privacy rights becomes increasingly necessary, as the individual will be gradually required to know how to behave in a digital environment, as required in the context of the analog world.

Throughout the analysis of the collected data, it was possible to perceive a pessimistic tendency on the part of the participants in relation to the availability of personal data, considering that most of the interviewees understand that handing over such data can bring risks. In addition, they also demonstrated the understanding that they have no control over the personal data that are made available. However, a considerable part of the public did not have the habit of reading the data consent terms before accepting them, demonstrating a contradiction between what the public thinks about the risks of providing their personal data and their everyday actions related to it. to this provision of information. With regard to the interviewed public's familiarity with the LGPD, it was possible to collect considerable information at all levels of understanding, given that most people claimed to have a basic degree of familiarity considering the General Data Protection Law.

Data collection for the present study proved to be limited to the interviewed public, most of whom were between 16 and 24 years old, had academic experience and lived in the Southeast region. For future

studies, it is recommended to investigate a larger population sample, together with a qualitative study to seek to better understand the contradiction presented, together with a better investigation of how individuals behave within the digital context based on their understanding of the LGPD.

REFERENCES

ABCOMM. **Faturamento do e-commerce cresce 56,8% neste ano e chega a R$ 41,92 bilhões**. 21 set 2020. Disponível em: https://abcomm.org/noticias/faturamento-do- ecommerce-cresce-568-neste-ano-e-chega-a-r-4192-bilhoes/.

ARKOSE LABS. **Fraud & Abuse Report Q2 2020**. Disponível em: https://www.arkoselabs.com/wp-content/uploads/Fraud-Report-Q2-2020.pdf. 2020.

Berghel, Hal. **"Malice domestic: The Cambridge analytica dystopia."** Computer 51.05 (2018): 84-89.

BRASIL, Comitê Geral de Internet. **Pesquisa web sobre o uso da Internet no Brasil durante a pandemia do novo coronavírus - Painel TIC COVID-19**. São Paulo: Cetic.br, 2021. Disponível em: https://cetic.br/media/docs/publicacoes/2/20210426095323/painel_tic_covid19_livro_eletr onico.pdf.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília, DF: Senado Federal: Centro Gráfico, 1988.

BRASIL.Lei 12.964/14, de 23 de abril de 2014. **Marco Civil da Internet**. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >.

Brasil. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, DF: Presidência da República; 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.

BRASIL. Lei nº. 8.078, de 11 de setembro de 1990. **Código de Defesa do Consumidor. Dispõe sobre a proteção do consumidor e dá outras providências**. Disponível em: http://www.planalto.gov.br/ccivil_03/Leis/L8078.htm

Breternitz, Vivaldo & Lopes, Fabio & Silva, Leandro. (2013). **O uso de Big Data em Computacional social Science: tema que a sociedade precisa discutir**. Revista Reverte - FATEC. 11.

CETIC. TIC COVID-19. **Pesquisa sobre o uso da internet no Brasil durante a pandemia do novo coronavírus**. Disponível em: https://cetic.br/media/docs/publicacoes/2/20200817133735/painel_tic_covid19_1edicao_ ivro%20eletr%C3%B4nico.pdf.

G1. **Megavazamento de dados de 223 milhões de brasileiros: o que se sabe e o que falta saber.** Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de- 223- milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml. Acesso em: 20 out. 2021.

Gordon, Sarah, and Richard Ford. **"On the definition and classification of cybercrime."** Journal in computer virology 2.1 (2006): 13-20.

Júnior, Severino Domingos da Silva, and Francisco José Costa. **"Mensuração e escalas de verificação: uma análise comparativa das escalas de Likert e Phrase Completion."** PMKT–Revista Brasileira de Pesquisas de Marketing, Opinião e Mídia 15.1- 16 (2014): 61.

Lozada, Gisele, and Karina da Silva NUNES. **"Metodologia científica."** Porto Alegre: SAGAH (2018).

Martin, Allan. **"A european framework for digital literacy."** Nordic Journal of Digital Literacy 1 (2006): 151-161.

MAYER-SCHÖNBERGER, Viktor; CUKIER, Kenneth. **Big data: como extrair volume, variedade, velocidade e valor da avalanche de informação cotidiana.** Rio de Janeiro: Elsevier, 2013.

NAGLI, Luiz Sérgio Dutra. **PANDEMIA NA PANDEMIA: A ESCALADA DE ATAQUES CIBERNÉTICOS** PÓS COVID 19. In: Anais do Congresso Transformação Digital 2020, São Paulo. Fundação Getulio Vargas.

Pinheiro, Patricia Peck. **Proteção de Dados Pessoais:** Comentários à Lei n. 13.709/2018- LGPD. Saraiva Educação SA, 2020.

RIBBLE, Mike. **Digital Citizenship in Schools**. 2. ed. Washington DC: International Society for Technology in Education, 2011. 150 p.

RIBBLE, Mike; BAILEY, Gerald. **Digital Citizenship in Schools: Nine Elements All Students Must Know**. 3. ed. Washington DC: International Society for Technology in Education, 2015. 222 p.

TAYLOR, Linnet. **What is data justice? The case for connecting digital rights and freedoms globally.** Big Data & Society, v. 4, n. 2, p. 2053951717736335, 2017.

Widup, Suzanne & Pinto, Alex & Hylender, David & Bassett, Gabriel & langlois, philippe. (2021). 2021 **Verizon Data Breach Investigations Report**.

Contatos: nathan-borges2011@live.com; fabio.lopes@mackenzie.com