User's perception about online personal data transmissibility

Pedro Pincho
Instituto Universitário de Lisboa (ISCTE-IUL), Portugal

Inês Messias
Instituto Politécnico de Santarém, ISTAR-Iscte, Portugal

Bráulio Alturas
https://orcid.org/0000-0003-0142-3737
Instituto Universitário de Lisboa (ISCTE-IUL), ISTAR-Iscte, Portugal

ABSTRACT

The usage of consumer's personal data is considered by companies as capable of creating immense value in terms of business. As such, the rise of using social networks to access users' shared information, gathering, processing and using it, in order to put together as much information as possible, has become a normal proceeding by companies that work in the sector, perceived as "new" actives for both companies and consumers. Thus, this data represents value to entities, that use them to reduce research costs to develop new products, as well as transactions costs while increasing their marketing incomes. Through personal information, the objective of this study is to determine what feelings are related to sharing personal data online, as well as variations in sharing it is intended for. The nature of the study is quantitative. The research questionnaire for this study was developed through a literature review, later shared on social networks, with 103 valid questionnaires having been collected. Data analysis was performed using IBM SPSS Statistics and excel programs. The results obtained allow us to understand what perceptions the population has regarding data sharing, suggesting that the individual perception of the transmissibility of personal data online is starting to be an area of interest for society, since there is a greater awareness of the dangers online, although this does not reflect a higher level of knowledge on the subject. The path to a more effective and efficient society has a certain price or consequence, namely our freedom and privacy.

Keywords: Data sharing, online privacy, online security, user trust, risk perception, Portugal

INTRODUCTION

By 2016 the internet had 3 billion users. 2 billion of them were social media users, and 890 million connected to Facebook daily (Aïmeur et al., 2016). According to a study developed by the same author (Aïmeur et al., 2016) when approached about their own perception concerning how their data was protected on social media, only 10% showed trust concerning social networks, 20% stated to trust e-commerce platforms and 22% answered to trust technology companies. A few of years later, in 2022, according to Statista (Buchholz, 2022) the active number of worldwide social media users is estimated at 4.6 billion, corresponding to 60% of the world's population. According to the same source, the projections show that this number is expected to rise by 6 billion in 4 years, by 2027. According to Zuboff (2020) we are living the Era of vigilance capitalism, whereas digital privacy has shown to be a growing concern to all. Understanding how this impacts users' individual perception of their own privacy management is a challenge (Soczka, 2014, in Zyboff, 2020).

On 2016, and to answer concerns regarding regulation of the use of social media and internet consumers' data, the EU has set the General Data Protection Regulation (GDPR) (2016/679), that has been active since 2018. This regulation is based in a proactive principle, whereas the responsible for data processing has to prove that all the phases of the data processing obeys to the regulation norms. Created to protect the citizens when it comes to how their information is treated, questions remain about the users' perception about this process.

The virtual hyper exposure noted by Weissman (2021) during the COVID-19 pandemic situation, has marked a transition considering how dependent society has become. The lack of alternatives makes users progressively more dependent on the use of internet for their daily tasks. With It, a growing concern surges, with a raising number of questions that is urgent to give answers to, were privacy and security are central when dealing with the consumers' perception of trust about the personal information shared on social media.

To better understand this issue, a study was made, based on 3 goals: 1) understand the feeling the consumer has when sharing personal information and data online; 2) deepen if the data sharing is in fact the path that should be followed, and if users are available in the future to share more data online as they do today; 3) understand if these approaches to data sharing, with all its pros and cons, are indeed beneficial. Focused on the transmissibility of personal data in the online context, this study had as main objective to understand how a user manages his/her personal data. The study's research question aimed to understand the users individual perception about the transmissibility of personal data in the online context. Hence, it aimed to 1) identify online shared information's sensitivity; 2) verify the level of satisfaction concerning GDPR; 3) determine the sensation while sharing data online; 4) identify key aspects to determine the construction of trust, in order to set an improvement strategy for the use of information systems to gather such data; 5) understand the perception of the advantages and disadvantages associated with sharing online data.

BACKGROUND

The reason for this study stems from the fact that the chosen theme is current and of extreme relevance to the business world, since it is a Portuguese national objective to empower business structures to achieve the third pillar of the goals stipulated in the 2030 horizon (Innovative Europe). To this end, it is necessary to have a full digital transition, in which the user is proficient in the use of technology in his daily life and professional context, thus enabling him to be a full citizen of the 21st century (European Commission, 2021).

This study also allowed us to better understand the Portuguese modern society in this new digital age, and to understand the influence that digital technology has especially on the lives of young people in this country.

As many processes can be listed in the course of human history, it is at this moment and context, absolutely fundamental to make the appreciation of one of the most complete, fast, intuitive and universal

tools: the Internet. Analyzing how the users perceive how data circulates on it, perceiving how they carry knowledge, dynamics, energies, dreams and ambitions to this environment.

Taking into account the current context, and the digital society in which we live today, it is important to understand the opinion of young people regarding the sharing of personal data online and whether they take into account a set of factors that underlie this issue, such as privacy, security or lack thereof. Moreover, we will try to understand how information systems can help in building trust about the sharing of personal data online.

As stated by Zuboff. S (2020), we live in the Age of surveillance capitalism. Digital privacy, has become a growing concern in the population, and there is a need for refined policies and regulation on this sector to ensure the individual privacy of citizens. "Surveillance capitalists know everything about us, yet their actions are unknown to us. They accumulate vast domains of new knowledge about us, but which is not intended for our use. They predict our future for the benefit of others." (Zuboff, 2020, p.26).

The inevitability of digital entering our daily lives has never been more evident, it remains for us to know how best to apply it. In a balance between options that will lead us to sustained and sustainable paths of development and evolution, it is important to keep in mind the risks inherent to an unbridled use, irresponsible or sustained in values that in no way dignify the human species.

With the growing number of data collected in scientific academic studies on this topic, it will be possible to have a better understanding of the externalities involved in this new world, thus extending the knowledge chain of this new disruptive business model that is data.

OBJECTIVES

Considering that theme of this dissertation focuses on the transmissibility of personal data in the online context, its aim is to better understand the relationship and the perception of the current digital society with the new world of data.

The main objective of this study was to understand how each individual manages his personal data. Data was collected in order to understand what feelings are inherent to sharing data online, and how proficiency in the use of information systems can create, or help to support, greater confidence to the users.

Thus, the research question was: "What is the individual's perception of the transferability of personal data online?"

The specific objectives of this study were:

1. Identify the sensitivity of information shared online;
2. Verify the degree of satisfaction regarding the standards in force for the protection of personal data;
3. Determine the existing sentiment during online data sharing;
4. Identify key points in building trust to define a strategy to improve trust of use based on information systems;
5. Understand the perception of advantages and disadvantages associated with online ata sharing;

As a Research function, it was intended to analyze the existing perception during the sharing of personal data online, taking into account the existing regulations in view of the risks of exposure, appreciation of inherent problems, difficulties, advantages and disadvantages in the operationalization originated through data sharing and the achievement of the proposed objectives. In the end, in a conclusive tone, essential points or key points are presented, for the creation of trust during the process of online data sharing.

LITERATURE REVIEW

Online privacy

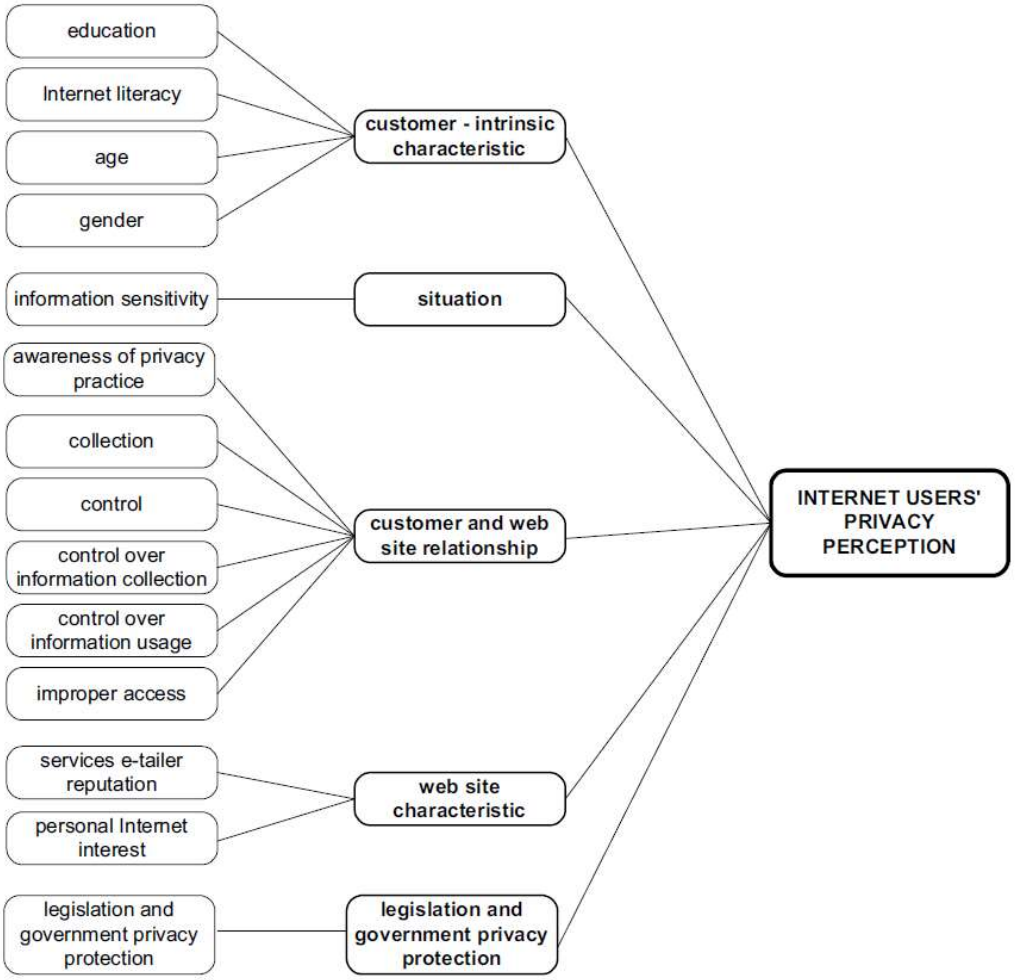
When online privacy, or the lack of it, is identified as one of the main negative factors about internet, Mekovec & Vrček (2011) confirm that its users have no trust about the guarantees that website owners offer while assuring that their personal information is to remain private. The notion

of privacy and the factors that influence the worries about privacy are therefore crucial to understand how users perceive it, to better understand how to avoid and resolve such issues.

Sheehan and Hoy (2000) were among the first to study online privacy concerns and they identified 3 factors that influence the users' concerns. Namely, control over capture and use of users information, short term operations, i.e. transactions, and the established relationship that approaches questions over client and website relations. The same authors suggest factors that can influence worries about online privacy: a) the consumer intrinsic characteristics; b) their perspectives, beliefs, and attitudes concerning marketing, the control of information mechanisms and processes to acquire data; c) website related variables; d) situational variables.

Showing the same concerns Mekovec & Vrček (2011) propose a model to study online privacy (C.f. Figure 1), based on 5 group of factors, that then subdivide in specific indicators: 1) consumers' intrinsic characteristics; 2) situational factors; 3) website characteristics; 4) the client's relationship to the website, and 5) governmental legislation and privacy protection.

Figure 1. Model proposed by Mekovec & Vrček (2011)



Besides online privacy, risk perception is also crucial to perceive when trying to establish how users understand data privacy concerns. Especially because the users' perceived risk when making the decision to share data online is directly related to its previous experiences. And it diminishes every time it shares information or shops online (Liebermann e Stashevsky, 2002).

The web and the corporate world

In the beginning, the Web invented by British scientist Tim Berners-Lee consisted of collecting text through HTML sites hosted on servers, when it appeared around 1989, being quite primitive if we consider the extraordinary progress that has taken place since then.

The web was primarily designed for sharing information between universities and science institutes.

Actually, the computational society is a new state of human civilization, a new way of involving the intensive use of information in all spheres of human activity, implying a severe impact both at a social, economic and environmental level. An example of this has been the recent use of teleworking, due to the pandemic caused by COVID-19, which has shown us the need for an urgent digital transition within companies and institutions, where everyone involved has the essential structures, resources and skills to do it. Moreover, the modernization of public services, health services, education, culture, environmental management, among others, has become increasingly urgent, where we can add new ways of communicating data and information between government institutions. and the population, in order to streamline processes and cross-reference data and information that allow reaching two more of the sustainable development objectives: the effectiveness of institutions, and partnerships for the implementation of the objectives.

The implementation of a digital economy does not in itself guarantee sustainable development, but it has a great impact on the quality of public life. The development of these new meanings of communication and technological information are an important factor in increasing economic competitiveness, opening up new perspectives regarding methods of organization and creation of new jobs.

However, human rights are not guaranteed, and are vital values in the new digital world, which is why it is important to create conditions for their preservation. From the point of view of Rafisovich et al. (2020), the true progress of humanity in this process of digital development is the capacity for self-development, the development of human consciousness and intelligence along with the improvement of moral qualities.

Jacksi & Abass (2019) indicate that many technologies are being used over the internet for document sharing, each with different characteristics, methods and protocols. However, for these authors, the most common and easiest to handle is the web, with few and simple features. According to the same authors, web developers want the machine to think more and more like humans, through the addition of new tools, methods and protocols, being able to define the web as a center for sharing information. Thus, the measurement of user confidence becomes essential, given the role that privacy and security in the handling of online platforms and websites represents so that the companies that own them can continue to collect information that makes it possible to benefit from the potential of convenience in relation to the information that they offer, simultaneously providing that the handling of their products can be done in a safer, clearer and more transparent way.

According to Chin et al. (2012), we must first of all understand users' attitudes towards smartphone security and privacy and how they may differ from attitudes towards computing systems. To improve the security of mobile systems, we must understand the challenges and concerns that users currently have with performing sensitive operations on their smartphones and identify opportunities to improve the security of systems.

Risk perception

If we consider Rafisovich et al. (2020), the world entered a new development phase, the Era of digital society, ruled by an unprecedented development when it comes to scientific knowledge and their constant usage, something that society has never seen before. This new stage of human development, were world economy and people living standards, have had great changes, much due to technological development. These new technologies that we now consider part of our daily lives, have been substituting and rendering others obsolete, growing naturally with scientific discoveries, resulting in the appearance of new professions and opportunities. Following this transformation Catalina, López-de-Ayala, & García, (2014), makes a new definition of risk perception as the “cognitive process that is based on the information that each person has about certain subjects (...), and that each one processes it by organizing their value

judgments", which will later conditions their behavior, making the perception of risk a fundamental factor in the acquisition and maintenance of actions related to cybersecurity, mainly as a shield against the present dangers, generally associated with unsafe behavior.

Knowing that the notion of risk perception changes as reality changes, Yap, J. B. H., & Ng (2018) states that the concept of risk has been explained by a set of academic disciplines, namely, sociological, cultural and psychological, in a study setting that considers environmental, individual and cognitive factors, capable of contributing to how risk perception varies. Rhaki Takur e Mala Srivastava (2015, p. 153) indicate that there are several studies that present online security as a key factor to understand users' attitudes when using web services. Considering this aspect fundamental when promoting integrity, confidentiality and authentication as well as not recognition of relationships.

According to Leblanc & Biddle (2012), when people choose to engage in an online activity, such as banking or shopping online, they are making a trusting decision about the provider of the website or application in question. The vast majority of users usually trust most if not all websites they encounter, causing significant security issues. Hence, any proposed solutions to reduce the threat of online attacks must include consideration of the psychological processes of end users, to improve the way users perceive the risks they are incurring when navigating online. Leblanc & Biddle (2012) also indicate that, in their study's main findings, users reported greater risks perception when associated with finance-related activities, such as banking and online shopping, but attribute lower risk perception to online activities such as using a search engine, or participation in social networks. Knowing that these networks are highly valuable targets for attackers, the risk of unsafe behavior to occur in these platforms is high.

The internet has led to a significant increase in the number of transactions and options for products and services (Zhuang et al., 2018). In this sense, there has been an increase in online commercial transactions in recent years (Raluca, 2018), despite the users' uncertainty regarding the quality of products. Kim and Krishnan (2015) refer that this is caused due to online transactions being more comfortable and perceived as a allowing them to saving time and money for consumers who make purchase decisions through this channel. This allows us to consider that the consumer's perceived risk in decision making is associated with elements related to previous experience and previous purchases, and that this perceived risk decreases as the consumer makes more purchases and goes through more similar shopping experiences (Liebermann and Stashevsky, 2002).

Hence, to minimize purchasing risks for customers, companies must show that they honor their commitments and serve consumers in the best possible way. As for online consumers, they must be offered multiple channels that offer information about these processes, in order to help them to choose knowing they are making the best decision about the channel they use.

Risk perception when using the web

Anderson et al. (2014), tells us that the internet is capable of providing an excellent forum to discuss any issues that may not be covered by traditional media. Having the potential to interconnect ideas, thoughts and goals of individuals, however far away they are. Even so, and despite all the positive aspects that web developments bring us, each of them has inherent risks, and it is important to check the perception that users have of the risks they run. Unprecedented amounts of information are shared today by people, appearing therefore new problems of scalability, integrity and availability of the information in the systems (Monteiro & Alturas, 2012).

Yap, J. B. H., & Ng (2018) advances that the concept of risk has been explained by a set of academic disciplines, namely, sociological, cultural and psychological, in a context of study considering environmental, individual and cognitive factors, capable of contribute to the perception of risk variation. Rhaki Takur and Mala Srivastava (2015, p. 153) indicate studies that present online security as a key theme to understand the user's attitude in the use of web services. This being fundamental for the integrity, confidentiality, authentication, and non-recognition of relationships. In the study carried out by these authors, consumers associate security risks with losing money. Heavily influenced by the imagination of stories about hackers, consumers believe that their online accounts are in danger of being accessed by third

parties without their consent, and that serious financial implications could ensue. The perception of the risk of privacy is defined by the possibility that, through online business, personal information may be used inappropriately, thus invading the consumer's privacy.

This personal information is largely forwarded to CRM (Customer Relationship Management) business processes, with the aim of optimizing your sales and service provision. CRM, according to Payne & Frow (2005, p. 168), is defined as a strategic approach aimed at increasing value for shareholders, through the development of relationships between entities and their main customers and customer segments, offering thus better opportunities for the use of data and information, so that they have a better understanding of both the customer and the implementation of relationship marketing strategies.

The definition of the concept of data and information is fundamental in approaching this topic, and can be defined as a set of symbols that represent a perception of raw facts, that is, and following Debons, Horne, & Cronenweth (1988), they are events from which inferences or conclusions can be drawn. Information is understood as the organization of data seeking to answer the following basic questions: What? Who? When ? Where?.

For Qi & Zhang (2012), the concepts associated with mass production, first created during the industrial revolution, are being replaced by new ideas where the relationship with the consumer is the center of the business. The focus should be on what the customer needs rather than adding features to products. The old "design-build-sell" model is becoming obsolete, giving rise to the "sell-build-design" model. This means that the cost associated with stimulating customers and acquiring new customers is much lower than previously practiced. In order to respond to this evolution, companies focus their attention on increasing the customer's business value through analysis, so that the customer can be monitored throughout their life cycle. For this, they use CRM systems, which analyze data using tools such as data warehousing, data mining, customer relationship management, statistics, among others, providing new business opportunities in view of the needs highlighted in the market. All these processes make CRM a process for managing the relationship between the business and the customer.

As Chen & Popovich (2003) refer, CRM is not merely a technological application for marketing, sales and services, because when successfully implemented, it is a multifunctional system, customer-oriented, where strategy and technology integrate in ways that maximize relationships and serve the entire enterprise. The development of Information Technologies and Data Science has enabled companies to understand and predict customer demand more accurately through quantitative approaches (Chong et al., 2017), also contributing to a constant increase in the automation of customer processes. traditionally human-based decision making (Miller, 2018). In this way, one of the conditions to start the CRM process is the possession of customer information, using data that already exists from existing customers, but also that can be acquired through data provided by external sources.

Data privacy protection legislation and norms

Regulation (EU) 2016/679, of the European Parliament and of the Council, of April 27, 2016 (General Data Protection Regulation – GDPR) applies in Portugal and in the other Member States of the European Union from 25 de Maio de 2018. Thus, establishing a principle of (pro)active responsibility, where the person responsible for the processing of personal data demonstrates that in all stages of the process, this treatment complies with the Regulation.

This regulation establishes the rules regarding the processing of personal data, of a person, company or organization, in the European Union (EU).

Presenting in the general provisions, the main objectives of its existence, namely:

1) Establish the rules regarding the protection of natural persons, with regard to the processing of personal data and the free movement of such data.

2) Defend the fundamental rights and freedoms of natural persons, namely their right to the protection of personal data.

3) Clarify that the free movement of personal data within the Union is not restricted or prohibited for reasons related to the protection of natural persons, with regard to the processing of personal data.

That said, the definition of personal data becomes fundamental for a better understanding of the subject in question, being defined as information relating to a natural person who can be identified or identifiable by means of an identifier, such as a name, an identification number , location data, or to one or more elements specific to the physical, genetic, mental or social identity of a natural person (European Commission, 2016). For the preservation and confidentiality of this information, it is extremely important that the individual decides what to do with their own personal data. This implies greater transparency, both in the relationship between companies and people, in the way their data is collected and processed. Goddard (2017), presents this concern about privacy in which the European Union has focused its attention, as an opportunity to raise awareness of populations regarding problems related to privacy. The researchers believe that policies related to privacy can bring about confidence in populations regarding the ethical treatment of data and also a global impact on the perception of these matters. Not only organizations within the European Union will feel pressure on new methods of applying data processing. Outside the European space, there will also be pressure, as they will have to ensure high GDPR standards reflected in contractual provisions.

It is also possible to add that the RGPD goes beyond the legal process associated with it, as it is also responsible for a normalization and organization of data processing that until now would not have been put into practice, indicates Goddard (2017). According to a study presented on the Statista platform, carried out in January 2021, and in response to the question about the perception of technology companies' control over consumers' personal data, 66% share the feeling that technology companies have too much control over your personal data. The same study reports that respondents in Spain, the United Kingdom and the United States had higher levels of concern about data control, but even those countries that appear to agree least with the statement show more than 50% agreement with over-control over their data. personal.

METHODOLOGY

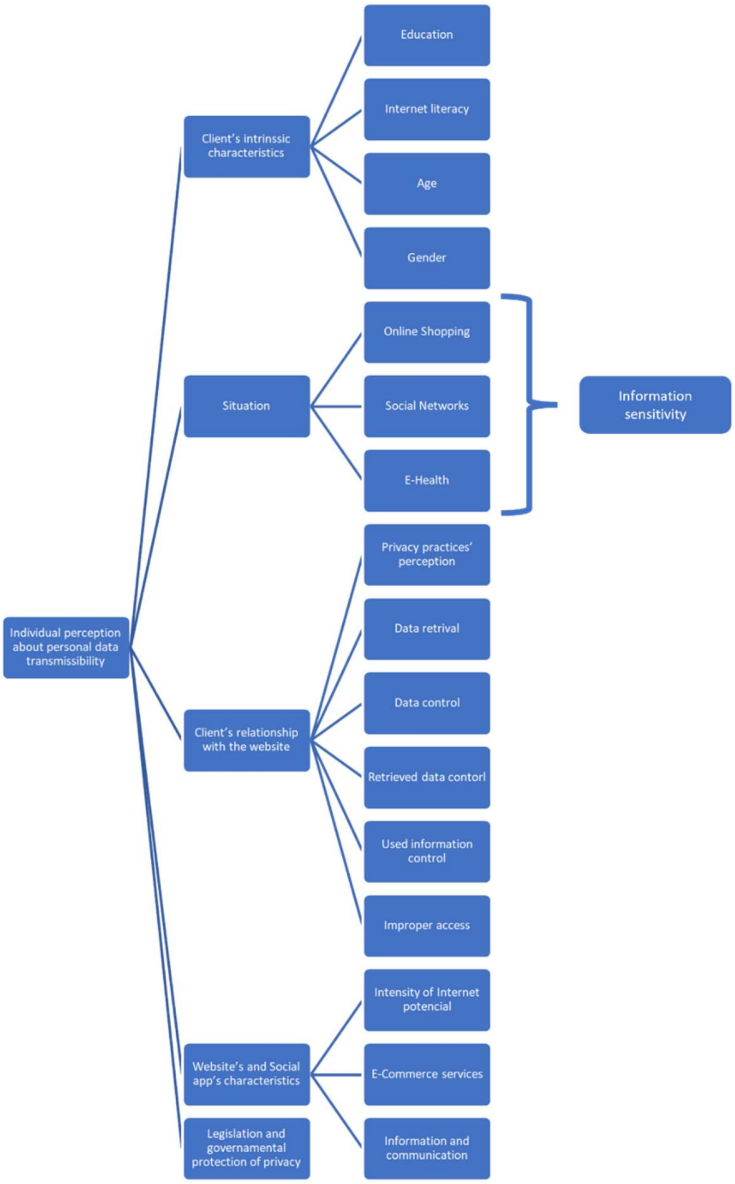
The study here presented in this paper had as goal to understand the feeling the consumer has when sharing personal information and data online, in order to deepen if the data sharing is in fact the path that should be followed, and if users are available in the future to share more data online as they do today. It also aimed to understand if these approaches to data sharing, with all its pros and cons, are indeed beneficial.

Hence, taking into account the objectives set for this study, a questionnaire was designed based on an adaptation of the Model proposed and validated by Mekovec & Vrček (2011) on their studies (C.f. Figure 2). The questions in this present study's questionnaire were created considering an adaptation of this model to the current technological context, and to the study's objectives. This adaptation of the model for this study considers the evaluation of the perception of privacy not only in the context of web pages, as in the original model, but also in the context of mobile applications, games and online purchases, trying to take into account factors that the previously analyzed authors during the literature review indicate as having an impact on individuals' perception of privacy, in the current digital context.

This study's questionnaire was composed by 7 sections, were the first group refers to the consumer's intrinsic characteristics; the second group aims to know the situation factors specific to the consumer's relationship with information technology (IT), including issues related to the usage of social networks; the third group aimed to know the consumer's relationship with the IT, specifically online shopping habits; the fourth group's goal was to know the specific situation factors concerning the usage of e-health apps; the fifth group aimed for a more generic knowledge about societal behavior concerning information systems in order to understand what are the specific areas were consumers feel more and less safe, as well as what are the prevalent feelings during the moments of data sharing online; the sixth group allowed to understand the characteristics of the websites that are most used/consulted; and the seventh group had the focus of getting to know the users' understanding about governmental privacy protection legislation and how this understanding influences their behavior when sharing data online.

Moreover, this questionnaire was subject to the appreciation of an expert in the field, as well as a non-expert, in order to validate the composition and see if it would be in accordance with the proposed objectives, together with the perception of it for readers before its release to the public.

Figure 2. Mekovec & Vrček (2011) model adaptation, about individual perception on data transmissibility of personal data online

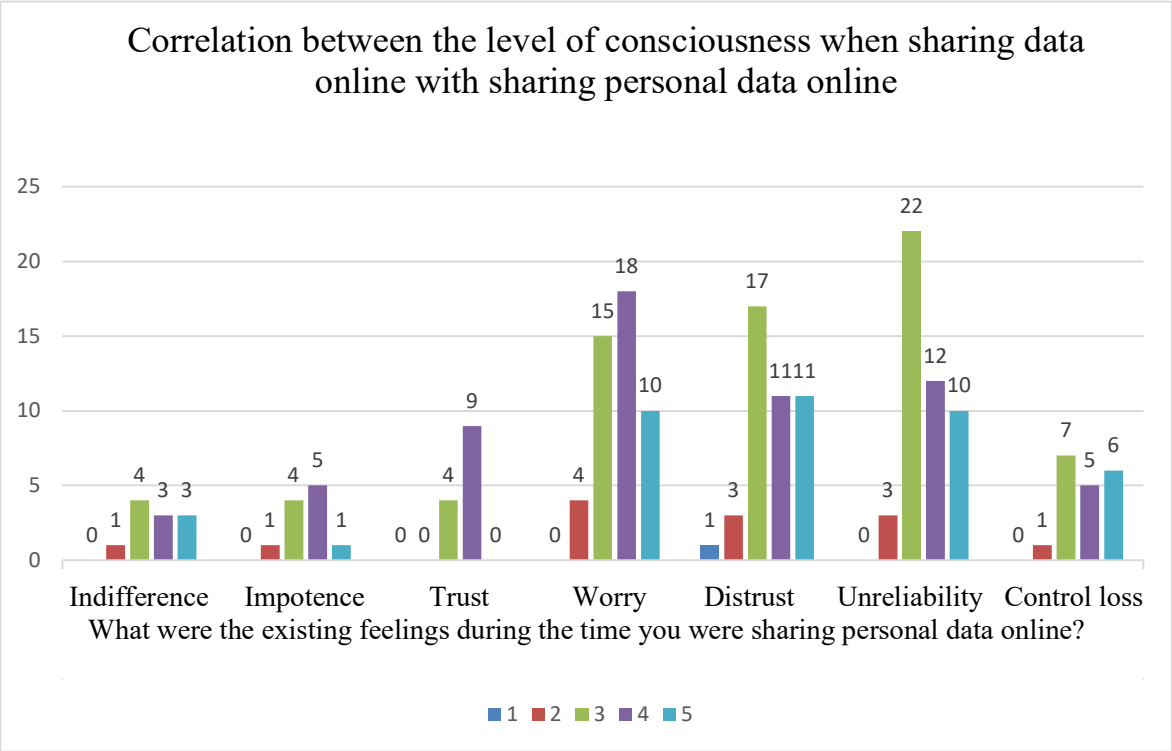


FINDINGS AND DISCUSSION

Considering the research objective and goals, this study's methodological approach included to design a questionnaire, that was implemented via social media. This data gathering instrument was designed considering an adaptation of Mekovec & Vrček model (2011) that was made to encompass today's online reality. The questionnaire's goal was to evaluate the users' perception about the privacy of the data they share online in today's digital context. After its design, the questions were valitated by an expert and a non-expert. It was of great importance to know the intrinsic characteristics of the consumer, because as Mekovec & Vrček (2011) advances, when approaching the subject of an individual's perception of privacy, it is important to consider the characteristics of that same individual, given that people share different perspectives, experiences and consequently opinions. To determine the existing feelings of this

study's enquiries when sharing personal data online, respondents were asked what feelings they had when sharing personal data online, where the most recurrent feelings were concern, insecurity and distrust. Through the correlation between the degree of awareness when sharing personal data online and what feelings exist while sharing data, it was possible to conclude that there is mostly a level 3 awareness level where it is also possible to observe that at this level of consciousness, there is a greater number of clicks, which in turn translates into a greater number of feelings existing during the sharing(C.f. Figure 3).

Figure 3. Correlation between the level of consciousness when sharing data online with sharing personal data online



Respondents were also asked about their level of loss of control over data already made available over time, and they were able to conclude that there is a high average perception of loss of control (72.8%). Questioned about the habit of reading the terms and conditions of security and privacy on websites and applications in order to understand the "rules of the game", the answers indicate that there is no frequent practice of reading them. Perhaps for this reason, the question regarding the frequency of adjustment of the definitions of the terms of privacy and security, also indicates that it is not a custom, as more than half of the sample (55.2%) indicate that they do it a few or sometimes. Correlating the qualifications of the respondents with the frequency of adjustment of the definitions of the terms of privacy and security, as shown in Figure 4, we can observe that the respondents do not adjust the definitions of the terms of privacy and security regardless of their qualifications. The highest concentration of responses in terms of frequency of adjustment of definitions of terms of privacy and security, focuses on grade 2.

Regarding transparency in the processing of personal data during the online shopping process, the results indicate that the majority (66.3%) consider the process transparent, evaluating it as having a high average of transparency. In order to identify key points in building trust in the use of information systems, questions were asked about the degree of confidence they feel in the ability to process personal data by companies that own social networking platforms and websites, where the result indicates a low average confidence (74.5%). Considering that the trust factor is an extremely important point for the relationship

between users and information systems, it can be deduced that they feel little confidence in the capacity of data processing by social network companies. When asked about the degree of confidence when making online purchases, the vast majority (80.3%) indicated a medium high level. It should be noted that it is possible to verify that there is a small difference between the trust attributed to social networks and the trust attributed to e-commerce, with e-commerce where users have greater confidence.

When analyzing e-commerce specifically, we tried to understand how safe respondents consider the online shopping process, with 77.7% of the sample responding considering the degree of security as medium high, thus seeing the online shopping process as safe for users. Even so, this degree of trust felt may originate from the lack of knowledge of several factors, leading to a false sense of security, which, as described by Leblanc & Biddle (2012), is observed when the vast majority of users, generally trust the majority, if not on every site it finds, causing significant security issues. In this way, it should be noted that despite the degree of confidence shown by users regarding the safety of online purchases, this feeling may have several factors, not just the in-depth knowledge of the possible risks during these processes.

With regard to the type of information made available on social networks, it was possible to observe that sharing the real name is the most expressive, together with the date of birth, family members and their relationships. In turn, the least expressive are the address and telephone number, denoting some care in sharing information considered sensitive by most users. As for the type of privacy settings adopted for social networks, the limitation to the public that can access the content is the most evident, together with alert checks for account handling on other devices and limitations on who can see the list. of friends. The least mentioned are search engines outside of social networks, the email or telephone number provided and location tracking. By correlating the participants' educational qualifications with the type of information available on social networks, we observe that the line corresponding to secondary education is where there is the highest concentration of responses, indicating that for individuals with this type of qualifications there is a greater amount of information available online, making these individuals the most exposed segment virtually.

Regarding the information available in online purchases, the real name, address, taxpayer number and email are the most shared information, while financial information and sharing the date of birth are the least considered. Through the correlation between qualifications and the type of information available in online purchases, it was possible to observe that the level of secondary education qualifications continues to be the most exposed segment, despite presenting a slight difference in relation to participants with graduation.

Concerning the sharing of personal data to use e-health apps, our inquires have stated to make available their name, email, number of steps they make during the day, height, weight and heart rate, considering them relevant data for the apps to function properly. The less shared information is relative to personal illnesses, assurance policy number, location, and address. When correlating this information and their academic qualifications, it was possible to conclude that graduates are the ones that share more data for e-health apps. Furthermore, comparing these findings with the other areas that were considered for this study, it is possible to conclude that it’s on e-health that users share more personal private data.

When analyzed the responses obtained regarding the pre-disposition of respondents to sharing personal data online on the various topics arranged, it was possible to conclude that the areas where respondents are less willing to share their personal data , were the areas of online games together with social networks, as they present a higher concentration of responses in a very low pre-disposition. If these were the two areas where there was less willingness, on the other hand, e-commerce, education and the professional context are the areas where there is greater availability for sharing personal data.

Thus, knowing the difficulty in measuring the perception or sensitivity of information shared online, and that it is described as individual privacy concerns for a specific type of information in a specific situation, it was possible to conclude that there is some sensitivity of information shared in Portuguese society, but that the path of instruction and development of digital literacy in our community is still a way to go, and the “seeds” of digital knowledge have been sown. It should be noted that internet users' perception of a website or the digital world depends not only on their current interaction, but also on the consideration of experiences with websites or past contexts.

Regarding the satisfaction level with personal data protection legislation and norms, most respondents were moderately/highly satisfied (73,8%). Correlating this with their academic qualifications it was possible to observe no variation, hence this satisfaction was verified independently of academic qualifications. When inquired about these norms effectiveness, the results were similar, with a slight variation on the moderate level, were 50% of the sample was. Hence, it is possible to conclude that there is a need to contextualize users about their privacy and online security rights, norms, and legislation, in order for them to feel safer.

To identify the key aspects to build trust in using information systems, respondents were inquired about their confidence level about the treatment companies do of their personal data. Results showed that respondents feel less trust when it comes to websites and social networks (74,5%). However, their level of trust on how e-commerce websites deal with their personal data, our respondents answered to feel they are very trustworthy. Hence, to find out more why this happens, our respondents have stated that they feel that the online shopping process is very safe, allowing to conclude that their level of trust can happen due to the lack of knowledge about several factors, leading to a false sense of security, as Leblanc & Biddle (2012) described.

As such, the presented level of trust by our respondents may have several factors, and not just their profound knowledge about the possible risks they incur into during these processes.

Comparing the level of trust attributed to the areas of social networks, e-commerce and health, we can conclude that social networks are the area where there is a lower degree of trust and the area of health where there is a higher degree of trust. As for their usage of social networking platforms, online shopping or health applications, we have that 99% of respondents use social networks, 88.3% shop online and 70.9% use health or physical exercise applications. Thus, it is possible to conclude that although people use social networks more in their daily lives than they shop online or use health or physical exercise applications, this does not mean that they feel more confident in the handling of their data by entities, holders of social media platforms and websites.

In order to identify key points in building trust with information systems, we can combine this information with the information available for the purpose of identifying existing feelings during data sharing (concern, insecurity and distrust) to seek combat them.

The way to build trust will be by providing information to the user in an open, clear and summarized way about the process of processing their data online. The strategy for improving user confidence involves educating society in handling its data online.

Understanding the perception of the advantages and disadvantages associated with sharing personal data online, we can conclude that in social networks, appreciation is indifferent or a practically remote advantage for about 68% of respondents. As for the usefulness of e-commerce, it appears that the majority (48.6%) consider it advantageous or very advantageous. Finally, in the health area, 57.3% answered that the applicability of sharing their personal data for health purposes is indifferent or advantageous.

In view of these results, we can conclude that there is a difference in the results of e-commerce, compared to social networks and health. Perhaps because in e-commerce there are more situational factors where the process unfolds in an efficient way, leaving the user satisfied for having made the purchase he intended. However, it should be noted that this analysis may not be being carried out at the level of the processing of personal data, but in the provision of the service.

The analysis of the results obtained allowed responding to all the objectives proposed in this study, having been supported by indicators that made it possible to support certain conclusions that help us to understand a little better the relationship of our society with the information systems that we currently have.

It is possible to highlight the fact that the respondents' educational qualifications are not a decisive factor for variations in the degree of satisfaction in relation to the prevailing norms. But that the level of contextualization in relation to the RGPD can be a differentiating indicator of the level of satisfaction with current regulations. It is important to mention the difference in society's willingness to share personal data online, depending on the area for which it is intended. That is, there are areas of our society where the population is more willing to provide more personal data, namely in the areas of e-commerce, education and professional context.

As for the existing feelings when sharing personal data online, we can conclude that the predominant feelings, as stated previously, are concern, insecurity and distrust.

This is a clear indicator that these could be the feelings or areas to be overcome in order to build trust in information systems. Following the analysis of the data collected in this study about users' trust, it is possible to infer that this is related to the way society interprets the handling of its data online. It is important to educate people in this regard and give them all the information they need while using websites, not putting information in small print, for example, in order to generate feelings that something is hidden or hidden beyond the information provided.

According to Chin et al. (2012), the measurement of users' trust privacy and security in the handling of online platforms and websites is extremely important so that the companies that own platforms and websites can have information that allows them to make the handling of their products safer, allowing users to benefit from the security and confidence in together with the convenience potential offered by online platforms and websites.

Finally, in order to understand the perception of the advantages and disadvantages associated with data sharing, we can conclude that society mostly considers the use of information systems in the areas of social networks, e-commerce and health to be advantageous.

Taking into account the digital world we live in, it is essential to consider the perspectives related to this topic in order to understand the impact that this new world can bring to our society. Namely, through the weighting of values, as the price to be paid for an effective and efficient society can lead to a lack of privacy for those who live in it. Over time, we will encounter situations where the invasion of privacy will prevail over personal interests, and then it will be important to have as much information as possible about our relationship as a society with information systems and how information systems manage to transform as a society, without affecting our individual freedom and privacy.

CONCLUSIONS AND RECOMMENDATIONS

It is a conclusion of this study that although people use social networks more in their daily lives than they shop online or use health or physical exercise applications, this does not mean that they feel more confident in the handling of their data by entities, holders of social media platforms and websites. In order to identify key points in building trust with information systems, we can add this information, to the one already available, in order to identify the feelings that exist during data sharing (concern, insecurity and distrust) to help combat them. The feeling of trust could be addressed by providing information to the user in an open, clear and summarized way about the process of processing their data online. The strategy for improving user confidence involves educating society in handling its data online.

More in-depth studies on the areas where there is a greater willingness to share personal data, could be an asset to complement the results of this study. Since a greater willingness to share personal data on a given topic must have a social foundation, normally associated with areas where greater efficiency is sought in the provision of services, such as “health”, even this is not a priority area for society according to this study.

The correlation of more variables could also enrich future studies, giving as an example the fact that the different generations that use information systems have different behaviors and preventive measures between them and understand the respective differences in these behaviors.

Another possible future topic of research would be to understand to what extent the intervention of the public or private power should be responsible for the security of the use of the network, in order to guarantee the confidentiality and integrity of the information available online, so that a relationship of trust can be built with transparency of information systems.

There are several paths that can and should be taken within this area of research. Suggesting a topic for future research, it could be about the price or consequences of a society that is more effective and efficient, through the crossing of data, and to what extent society would or would not be willing to give up its data.

ACKNOWLEDGMENT

Any acknowledgment to fellow researchers or funding grants should be placed within this section.

REFERENCES

Aïmeur, E., Lawani, O., & Dalkir, K. (2016). When changing the look of privacy policies affects user trust: An experimental study. Computers in Human Behavior, 58, 368-379.

Buchholz, Katharina (2022). The Rapid Rise of TikTok .Statista, Topics – Social media. https://www.statista.com/chart/28412/social-media-users-by-network-amo/

Catalina-Garcia, B., López-de-Ayala, M.C., & García, A. (2014). Los riesgos de los adolescentes en Internet: los menores como actores y víctimas de los peligros de Internet [The risks of teens on the Internet: minors as actors and victims of Internet dangers]. Revista Latina de Comunicación Social, 69, 462-485. DOI: https://doi.org/10.4185/RLCS-2014-1020

Chen, I. & Popovich, K. (2003). Understanding customer relationship management (CRM) People, process and technology. Business Process Management Journal 9(5), 672-688.

Chin, E., Felt, A. P., Sekar, V., & Wagner, D. (2012). Measuring user confidence in smartphone security and privacy. SOUPS 2012 - Proceedings of the 8th Symposium on Usable Privacy and Security, 1. DOI: https://doi.org/10.1145/2335356.2335358

Chong, A., Ch'ng, E., Liu, M., & Li, B. (2017). Predicting consumer product demands via Big Data: the roles of online promotional marketing and online reviews. International Journal of Production Research, 55(17), 5142-5156. DOI: https://doi.org/10.1080/00207543.2015.1066519

Debons, A., Horne, E., & Cronenweth, S. (1988). Information science: An integrated view. Boston; G.K. Hall; 1988. 172 p. graf. (Professional Librarian Series).

European Commission (2021). Horizon Europe, pilar III - Europa inovadora – Apoiar e estabelecer ligações entre os inovadores na Europa. Publications Office of the European Union Directorate. General for Research and Innovation https://data.europa.eu/doi/10.2777/831048

European Union (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016. Practices for Public Administration on the General Data Protection Regulation (GDPR). Available at: https://www.sg.pcm.gov.pt/media/33595/05.pdf

European Union (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and the free movement of such data. Official Journal of the European Union. Available at: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&qid=1641839336270&from=PT

Gapsalamov, A. R.; Bochkareva, T. N.; Akhmetshin, E. M.; Vasilev, V. L., & Anisimova, T. I. (2020). Sociedade digital: Novos desafios para a educação [Digital society: New challenges for education]. Periódico Tchê Química; 17(34), 803–817. DOI: 10.52571/PTQ.v17.n34.2020.827_P34_pgs_803_816.pdf

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. International Journal of Market Research, 59(6), 703-705.

Jacksi, K., & Abass, S. M. (2019). Development history of the world wide web. International Journal of Scientific and Technology Research, 8(9), 75–79.

Kim Y, & Krishnan R (2015). On product-level uncertainty and online purchase behavior: an empirical analysis. Management Science, 61(10), 2449-2467. DOI: https://doi.org/10.1287/mnsc.2014.2063

LeBlanc, D., & Biddle, R. (2012). Risk perception of internet-related activities. IEEE 2012 Tenth Annual International Conference on Privacy, Security and Trust, 88-95.

Liebermann Y, Stashevsky S (2002). Perceived risks as barriers to Internet and ecommerce usage. Qual Mark Res 5(4), 291–300

Mekovec, R., & Vrček, N. (2011). Factors that influence Internet users' privacy perception. IEEE Proceedings of the ITI 2011, 33rd International Conference on Information Technology Interfaces, 227-232.

Miller, A. (2018). Want Less-Biased Decisions? Use Algorithms. Harvard Business Review

Monteiro, D., & Alturas, B. (2012). Segurança e Privacidade na Web 2.0: Foco nas Redes Sociais [Web 2.0 Security and Privacy: Focus on Social Networks]. Egitania Sciencia, 10, 109-133.

Payne, A. & Frow, P. (2005). A Strategic Framework for Customer Relationship Management. Journal of Marketing 69(4), 167-176.

Qi, L., & Zhang, S. (2012). The Development of Customer Relationship Management System Based on Rough Set. Communications in Computer and Information Science, 315, 328–333. DOI: https://doi.org/10.1007/978-3-642-34240-0_43

Sheehan, K.B.; Hoy, M.G. (2000). Dimensions of privacy concerns among online consumers. Journal of Public Policy & Marketing, 19(1), 62-73. Sage Journals. DOI: https://doi.org/10.1509/jppm.19.1.62.16949

Soczka, L. B. D. C. (2014). Gestão da privacidade em redes sociais: percepções de uso de dados e partilha de informação pessoal. Dissertação de Mestrado, Universidade de Lisboa. Instituto Superior de Economia e Gestão. DOI: http://hdl.handle.net/10400.5/12689

Thakur, R., & Srivastava, M. (2015). A study on the impact of consumer risk perception and innovativeness on online shopping in India. International Journal of Retail & Distribution Management, 43(2), 148-166. DOI: https://doi.org/10.1108/IJRDM-06-2013-0128

Weissman, J. (2021). The Crowdsourced Panopticon: Conformity and Control on Social Media. Rowman & Littlefield Publishers. ISBN: 978-1-5381-4431-2.

Yap, K.W., & Selvaratnam, D. P. (2018). Empirical analysis of factors influencing the public health expenditure in Malaysia. Journal of Emerging Economies and Islamic Research, 6(3), 1-14. DOI: https://doi.org/10.24191/jeeir.v6i3.8783

Zhuang H., Leszczyc P.T.L.P., Lin Y. (2018). Why is price dispersion higher online than offline? The impact of retailer type and shopping risk on price dispersion. Journal of Retailing, Elsevier, 94(2), 136–153. DOI: https://doi.org/10.1016/j.jretai.2018.01.003

Zuboff, S. (2020). A Era do Capitalismo da Vigilância. A Disputa por Um Futuro Humano na Nova Fronteira do Poder [The Age of Surveillance Capitalism. The Struggle for a Human Future on the New Frontier of Power]. (1ª ed) Relógio D'Água Editores. ISBN: 9789897830907.

ADDITIONAL READING

Alturas, B. (2022). Introdução aos Sistemas de Informação Organizacionais - 2ª Edição [Introduction to Organizational Information Systems - 2nd Edition]. Edições Sílabo.

Whitman, M. E., & Mattord, H. J. (2021). Principles of Information Security (MindTap Course List), 7th edition, Cengage Learning.

KEY TERMS AND DEFINITIONS

Data sharing: Data sharing is the ability to make the same data available to one or many consumers. Nowadays, the ever-growing amount of data has become a strategic asset for any company. Sharing data - within your organization or externally - is an enabling technology for new business opportunities.

Online privacy: Online privacy is the level of privacy protection an individual has while connected to the Internet. It covers the amount of online security available for personal and financial data, communications, and preferences.

Internet security: Internet security is a term that describes security for activities and transactions made over the internet. It's a particular component of the larger ideas of cybersecurity and computer security, involving topics including browser security, online behavior and network security.

Social media: Social media refers to digital platforms and tools that allow users to create, share, and exchange content, opinions, and information with others. Social media platforms enable users to connect with each other and engage in online communication, which can include text, images, videos, and other types of multimedia.