UNIVERSIDADE DE SÃO PAULO
Faculdade de Economia, Administração e Contabilidade
Bacharelado em Administração

ANA HELENA FREITAS KUZNETZOW

Data security and value creation for consumers: Evidence from the United States

São Paulo/SP
2021

ANA HELENA FREITAS KUZNETZOW

Data security and value creation for consumers: Evidence from the United States

Trabalho de conclusão de curso apresentado à disciplina Trabalho de Conclusão de Curso II – EAD 0601, como requisito para graduação no Curso de Administração da FEA/USP.

Orientador: Prof. Dr. João Maurício Gama Boaventura

São Paulo

2021

Dedico este trabalho aos meus pais, minhas irmãs, ao meu padrinho e ao Murillo, com amor, admiração e gratidão por seu apoio, carinho e presença ao longo do período de elaboração deste trabalho.

AGRADECIMENTOS

Aos Profª Drª João Maurício, pelos ensinamentos, os quais contribuíram para meu crescimento científico e intelectual na elaboração deste trabalho.

A Helna, pela atenção e apoio durante o processo de construção deste trabalho.

À Faculdade de Economia, Administração e Contabilidade da USP pela realização do curso e por todas as oportunidades que me foram apresentadas por seu intermédio.

A todas as entidades estudantis pelas quais fiz parte, Cursinho FEA USP, Centro Acadêmico Visconde de Cairú, Associação Atlética Visconde de Cairú, PET ADM. Cada uma delas me ensinou algumas das mais preciosas lições universitárias

Ao Handebol Feminino FEA USP, por me trazer experiências maravilhosas e inesquecíveis durante a faculdade e por me ensinar que competir junto a amigas é mais valioso do que o resultado da competição em si. Ao Futsal Feminino FEA USP, por ter me ensinado tanto sobre comprometimento, dedicação e sobre o valor da vitória. E, por fim, ao atletismo, por ter me acolhido e ter me feito voar em solo firme.

RESUMO

Este estudo procura entender quais as melhores práticas relacionadas à proteção de dados que criam valor na percepção dos consumidores. Na Teoria dos Stakeholders, há debates sobre a relevância das questões éticas dentro do contexto da gestão de dados, contrapondo o benefício do maior conhecimento sobre os usuários, com a alta responsabilidade da gestão de dados dos consumidores. Além disso, existe a preocupação de como as empresas lidam com a proteção de dados na prática, na medida em que as empresas que não dão prioridade ao tratamento ético dos consumidores, podem gerar menos criação de valor na sua percepção. Assim, este estudo visa analisar as práticas abordadas sob a ótica da privacidade de dados que entregam valor aos consumidores. Para tal, será aplicada uma abordagem quantitativa e qualitativa a fim de analisar, juntamente com variáveis da Privacidade dos Clientes, como por exemplo, a venda de dados de clientes, rastreio da atividade do utilizador, controle do utilizador sobre a retenção de dados, violações da segurança de dados dos utilizadores e controvérsias sobre a privacidade dos dados, utilizando sempre uma abordagem descritiva no que diz respeito aos consumidores. Na abordagem quantitativa, se utiliza da função estática descritiva da base de dados da JUST Capital 2020 com 922 empresas, as quais foram divididas em 6 agrupamentos industriais. Já na abordagem qualitativa, foram analisados estudos fornecidos pela NSFOCUS, bem como a base de certificação da ISO 27002 e os relatórios públicos das empresas mais bem ranqueadas segundo a Just Capital, por segmento de indústria. Esta estratégia é adotada a fim de promover insights, entendimento de oportunidades e proposições de estudos futuros sobre a proteção de dados. Este estudo contribui para a literatura de criação de valor na gestão dos stakeholders, investigando a percepção do valor dos consumidores no que diz respeito à proteção de dados, expondo tanto o grau de importância que os consumidores atribuem a esta questão, por meio dos resultados da JUST Capital, como também as possíveis consequências que recaem sobre o comportamento das empresas. A análise de padrões encontrados nas práticas empresariais sobre o tema também auxilia no maior foco dado a crescente discussão da privacidade de dados. Além disso, o trabalho expõe uma nova visão de categorização das métricas da base da JUST Capital, a qual pode ser útil para outros trabalhos. A originalidade deste estudo reside na análise empírica da percepção de valor dos consumidores, relativo às variáveis de privacidade de dados, considerando algumas das maiores empresas no mercado mais expressivo do mundo, enquanto contribui para a validação da utilização de uma nova e promissora base de dados na investigação científica.

Keywords: Teoria dos Stakeholders, Criação de valor, consumidores, Proteção de dados, Big data.

ABSTRACT

This study seeks to understand which best practices related to data protection create value in the perception of consumers. In the Stakeholders Theory, there are debates about the relevance of ethical issues within the context of data management, contrasting the benefit of greater knowledge about users, with the high responsibility of managing consumer data. In addition, there is a concern about how companies deal with data protection in practice, as companies that do not prioritize the ethical treatment of consumers can generate less value creation in their perception. Thus, this study aims to analyze the practices addressed from the perspective of data privacy that deliver value to consumers. To this end, a quantitative and qualitative approach will be applied in order to analyze, together with Customer Privacy variables, such as the sale of customer data, tracking of user activity, user control over data retention, breaches user data security and data privacy disputes, always using a descriptive approach with regard to consumers. The quantitative approach uses the static descriptive function of the JUST Capital 2020 database with 922 companies, which were divided into 6 industrial groups. In the qualitative approach, studies provided by NSFOCUS were analyzed, as well as the ISO 27002 certification basis and the public reports of the best ranked companies according to Just Capital, by industry segment. This strategy is adopted in order to promote insights, understanding opportunities and proposals for future studies on data protection. This study contributes to the literature on value creation in stakeholder management, investigating the perception of consumer value with regard to data protection, exposing both the degree of importance that consumers attach to this issue, through the results of JUST Capital, as well as the possible consequences that affect the behavior of companies. The analysis of patterns found in business practices on the subject also helps in greater focus given the growing discussion of data privacy. In addition, the work exposes a new categorization view of JUST Capital's base metrics, which can be useful for other works. The originality of this study lies in the empirical analysis of consumer value perception, related to data privacy variables, considering some of the largest companies in the most expressive market in the world, while contributing to the validation of the use of a new and promising database in scientific research.

Keywords: Stakeholder Theory, Value Creation, Consumers, Data protection, Big data.

LIST OF FIGURES

LIST OF GRAPHICS

LIST OF TABLES

SUMMARY

1. INTRODUCTION

Value creation is the core premise of the purpose of business. This is the premise supported by the Stakeholder theory that influences business strategy, both in the academic field and in the practical aspect of business. “Stakeholders are any group or individual who is affected by or can affect the achievement of an organization’s objectives” (Freeman, 1984, p. 46). According to Harrison and Wicks (2013), regardless the type of stakeholders, such as consumers, workers or suppliers, firms should focus on attending stakeholders’ interests and treating them with fairness, as it influences a firm to create value and consequently, improve its performance (Donaldson & Preston, 1995; Freeman, 1984); (1994; Freeman, Harrison, and Wicks, 2007; Harrison, Bosse& Phillips, 2010; Jones, 1995; Jones & Wicks, 1999).

The concept of value in this context is a topic of discussion that several authors have addressed the subject with different approaches. In this paper, it will be used the same value concept that Soares (2014) uses, that is “a combination of results tangible and intangible assets that a company distributes to its stakeholders that satisfy its demands for maintaining the relationship between the company and the stakeholder” (Soares et al., 2014).

In the stakeholders’ literature, there are debates about the relevance of ethical issues in big data analytics and how consumers perceive the security of their data as a tangible value. According to Someh (2019), the non-reciprocal character of the interaction between organizations that deploy the technology, individuals and society puts in evidence ethical concerns or dilemmas for the different stakeholders in a context that these organizations have the power from collection to sale of individuals data, without the consumer's consent or awareness (Barocas&Nissenbaum, 2014; Solove, 2013).

Corporations perceive big data as a tool for commercial advantage, since they are able to survey the tastes and habits of their consumers more precisely. The potential negative outcomes enabled by big data extend far beyond the individual, into social, economic, and political realms, having its origins in the improper exploitation of its consumers' data (Wigan & Clarke, 2013).

Considering the growing importance of the topic of data management, ISO 2700 was created as an international guideline, which contains a series of standards that enterprises should follow in order to improve the security targets in general (Meriah&Rabai, 2019). This paper will focus only on virtual data security and it will be used some of ISO 27000 principles, such

as confidentiality, integrity, authenticity, availability for the choice of data security metrics provided by JUST Capital (2020) analyzed from consumers' perspective.

There is a concern of how companies adopt practices to deal with data protection. This paper seeks to analyze this considering that customers understand a company's reputation on factors related to how it treats its customers, including (1) protecting customer privacy, (2) treating customers fairly, (3) making products that do no harm, and (4) communicating transparently (JUST Capital, 2020).

The use of data has become a global trend, so that the study of consumer perception on this front is essential both from the social point of view, as from the business point of view, which, in theory, has its performance linked with the perception of value creation of its stakeholders. Therefore, companies that do not pay attention to ethics in relationship with their consumers may generate less value.

This research aims to answer the following question: What are the best practices of data protection that create value for consumers? In order to answer it, the JUST Capital 2020 database will be used as an important source of data and consumer research about American companies, allowing the search result to be achieved. Therefore, will be possible to analyze what practices related to data protection are the best to create value for consumers, generating evidence of the relevance of this topic amidst a context in which data sharing is becoming increasingly frequent.

2. THEORETICAL FOUNDATION

Next, in order to provide the study with a solid theoretical basis, stakeholder theories and the development of the topic of value creation will be addressed. Moreover, we discuss the topic of stakeholder theory, value creation, big data and data protection.

2.1 Stakeholder Theory

"Stakeholder theory is a tool to better describe the world and foster better action" (Parmar et al., 2010, p. 409) and in agreement with these lines, it came to address three interconnected problems relating to business:(1) the problem of value creation and trade (2) the problem of ethics of capitalism and (3) the problem of managerial mindset. To deal effectively with these problems, stakeholder theory suggests the unity of analysis between a business and the groups and individuals who can affect or be affected by the organization (Freeman, 1984).

The most used definition of stakeholder created by Freeman (1984) mentioned above brings, at first, a unified definition for stakeholders. Although, according with Parmar (2011), there are also searches that differentiate primary and secondary stakeholders' concept. The first refers to groups whose support is necessary for the firm to exist, and to whom the firm may have special duties. The second, refer to stakeholders who have no formal claim on the firm, and management has no special duties about them; nevertheless, the firm may have regular moral duties, such as not doing them harm (see for instance:Carroll & Bucholtz, 1993; Gibson, 2000). In this research, this differentiation is considered, and the focus will be on the primary stakeholders, more precisely on the customers.

In the literature there are debates about how managerial actions have the potential to affect a broad range of people all over the world (Clement, 2005) and how managers must be concerned about the responsibilities of the firm, as it affects not only the firm, but also its stakeholders as a whole (Parmar et al., 2010). Freeman (1984) also draws attention to the fact that companies must align social and ethical issues with the business model of the company and that any change in the management direction should consider the impact that will be caused on stakeholders (Freeman, 1984).

For that matter, the stakeholder management requires a deep commitment by the firms. According to Tantalo (2014), it can be divided into four steps: first, it is important to identify

the relevant stakeholder groups, second, it is necessary to ponder the relevance of each stakeholder, then understand how the expectations of each group are being met and finally, modify corporate polices if necessary, considering the stakeholders' priorities (Freeman, 1984). In this way, the company can more deeply understand the needs, as well as get closer to the variables that make up the value creation of its main stakeholders (Harrison et al., 2010).

Therefore, the stakeholders' perception of value must be examined carefully and, to bring benefits both to the company and to society indirectly, it must follow a process in which the stakeholder is placed at the center of management decisions, as was mentioned above. Next, we address in more depth the topic of value creation in this context and how it relates to the variables that we analyze in this paper.

2.1.1 Value creation

Freeman (2010) defends that "The primary responsibility of the executive is to create as much value as possible for stakeholders" (Freeman, 2011, p. 2). The importance of value creation generated by companies for their stakeholders is not limited to Freeman's research, by contrast, has repercussions in several research in the stakeholder's literature. Verbeke, Osiyevskyy and Backman (2017, p. 685), for example, argues that value creation is a fundamental prerequisite for the very survival of any company.

This statement requires a profound understanding of the definition of value creation. In the literature, however, there are several articles with different definitions of "value". Adam Smith analyzes the definition of value from a neoclassical and economic point of view, outlining subjective and negotiable characteristics for the term. Kant, on the other hand, details the definition of value opposing intrinsic and extrinsic value, as is evidenced in the table below. Another definition worth mentioning in the study is the one opposing subjective and objective value, and finally, the characterization of value by classifying it as tangible and intangible.

Table 1 - Different Value Definitions

Type of value	**Definition**

Value in Exchange	the idea that value is based on how much a given item is within a marketplace exchange (e.g., Adam Smith; Neoclassical Economics). Value here is negotiated and inter-subjective.
Intrinsic vs. Extrinsic Value	one way to think about value is whether it is intrinsic, or an inherent feature, of an item—or whether it is simply a vehicle or means to some other good (i.e., extrinsic). Most goods in the marketplace are "extrinsic." A sandwich is good for satisfying my hunger; money helps me feel important or secure—both are "extrinsic" goods. However, some things are good in and of themselves. Kant calls a good will an inherent good; virtues also would qualify as inherent goods
Subjective vs. Objective Value	e: related to the distinction between intrinsic and extrinsic good is the contrast between subjective and objective notions of value. While there are numerous ways of defining both terms, subjective typically refers to the assessment of an individual and what they happen to like, while objective typically refers to a norm that operates across individuals or at a higher level of analysis (e.g., a universal moral norm; a social value; a human right).
Customer Value – Tangible vs. Intangible	Products with Quality and Functionality, Product's Price, Perceived Quality, Service, Safety, Value for Money, Accessibility - time required to purchase the product and time required to master using the new product (Harrison and Wicks, 2013; Tantalo and Priem, 2016: 322; Clarke, 1998). Business Reputation, Respect, Environmental Corporate Responsibility and "Eco Friendly" Product (Harrison and Wicks, 2013; Tantalo and Priem, 2016: 322; Clarke, 1998).

Sources: Adapted from Boaventura et al., (2009), (2020) and Harrison & Wicks, (2013).

As this paper aims to discuss the consumer's point of view, it uses the definition of value creation with focus on customer' perspective from the table above, focusing on values such as safety, respect, business reputation, accessibility and considering that customers represent, within the universe of primary stakeholders, those who have greater strategic importance,

greater value and power over the company (Boaventura et al., 2020). Therefore, as much as the other definitions serve as a complement to the understanding of value creation, the most relevant definition for this study, however, is from Boaventura et al. (2020). In his research, different terms related to all the primary stakeholders' perception of value performed by companies was compiled and divided between tangible and intangible values.

Applying this understanding of value, it is possible to understand in more depth how the data security metrics discussed later in this paper relate to consumers' perception of value. Thus, this study contributes both to future research and to greater assertiveness in the management of companies, since, according to Priem (2007), when value is created the consumer (1) will be willing to pay for a novel benefit, (2) will be willing to pay more for something perceived to be better, or (3) will choose to receive a previously available benefit at a lower unit cost, which often results in a greater volume purchased. So, from the consumers' perspective, value creation involves increasing use, value or decreasing exchange value (Priem, 2007).

2.2 Big Data and Data Security

The term "Big Data" was first introduced in 2005 by Roger Magoulas for the purpose of defining a great amount of data that traditional data management techniques are not able to process due to its complexity and size (Chaorasiya& Shrivastava, 2014). For MIKE 2.0, a methodology which provides a framework for information management, Big Data is defined by its size, comprising a large, complex and independent collection of data sets with the potential to interact.

Given this intrinsic complexity of big data, both in literature and in practice, the study of algorithms has intensified, in search of a faster and more assertive use of data (Madsen, 2015). According to Gunther (2017), "algorithmic processing generally follows fixed, pre-programmed procedures" (Günther et al., 2017, p. 196) and it can provide patterns and insights that had not been considered before and can therefore change the course of management decisions.

On the one hand, the use of big data has its advantages, such as enhance customer satisfaction by using information from call centers and getting a pattern from it, improving services and products by knowing the potential consumers and their preferences. This is only possible because algorithms are increasingly capable of predict human behavior and the impacts

of that encompass both the individual sphere of consumers, who can have the service and products adjusted according to their preferences, but also the organizational sphere that, knowing the taste of its consumers, can focus its efforts more assertively and efficiently, being able to distribute value to its consumers more accurately (Boaventura et al., 2020; Günther et al., 2017).

On the other hand, there are debates on the literature if data management, especially regarding consumers' personal data, if it generates in fact only positive externalities for society and individuals. Zwitter (2014) in his study highlights cases of privacy breaches, extensive individual profiling and discrimination against customers and in line with this idea, "ethical issues arise when organizations collect, analyze, share, and/or sell individuals' data without individuals' genuine consent or awareness" (Someh et al., 2019, p. 720). In these cases, it is plausible to state that the proportion of the damage affects unequally consumers and institution, being the consumers the most affected in this case, since they are the owners of the data.

In the modern world, the internet and digital technologies have played a key role in business decisions, turning the ability to manage data into a core capability the same time that its relevance also increased in the field of corporate social responsibility. Gunther (2017) draws attention to two cases, Netflix who offers media streaming and built a dynamic of recommendations based on consumers' patterns and The New York Times, a newspaper which is now using data to engage readers in its digital environment. According to his research, those two cases are examples of this movement of monetization of personal data, in which have consequences for the company, for being inside its business model, but also transforming the customer experience.

The implications of these dynamic go beyond economic gains, but it can have a direct impact on consumers' data autonomy and privacy (Orbik&Zozul'aková, 2019). According to BBC, this impact was felt by nearly 339 million customers, who had their personal data, such as name, phone, email, passport and even credit cards exposed to a group of hackers who invaded Marriot International. A hotel company, which has international operations, was originally invaded in 2014, however the breach was identified in 2018. As a result, the company was fined €18.4 million for the violation by the UK's privacy control and has become one of the most emblematic cases of data leakage. EasyJet company also suffered from a cyber-attack that exposed sensitive data such as personal and payment information to nearly 9 million users, in May 2020 (NSFOCUS, 2019). In 2018, C&A, a Brazilian clothing retail company, also

suffered from cyber-attacks conducted by hackers. In this occasion, names, credit cards, personal codes and emails of 2 million consumers were exposed, this case makes it clear that the issue of cybersecurity is global and should be looked at carefully by all countries and companies that deal with data management

Understanding the growing relevance of data in recent years, The Economist argues in its 2017 edition that the world's most valuable resource was no longer oil, but data. ISO (The International Organization for Standardization) and IEC (International Electro technical Commission) also saw this growing importance and, in 1995, created a group of standards that govern the guidelines related to the scope of information security, being represented by the ISO 27000 series. This group includes ISO/IEC 27002, last revised in 2013, an international standard that establishes guidelines to support the implementation and control of the Information Security Management System (SGSI) in organizations (ISO/IEC, 2013). This standard contains 14 security control clauses containing 35 main security categories and 114 security controls which include technical measures such as cryptography or communication security (ISO/IEC, 2013), below are the 14 clauses of the document.

The standard established by ISO ensures that companies and their stakeholders are assured of safety and protected against harm, generating value to the business (ISO/IEC, 2013). In order to analyze the best practices, based on ISO, the 14 clauses were separated into 4 main pillars actions that companies should pay attention to:

Figure 1 - Four pillars of data protection

Four pillars of Data protection	14 Control Clauses of ISO 27002	Definition of the Clauses
Establishment of Privacy Policies and documentation	Information Security Policies	Information security should be directed from the top of the organization, and policies should be communicated clearly to all employees.
	Organization of Information Security	A management framework should support the organization's information security operations, both on- and off-site.
	Information security aspects of business continuity management	Information security continuity should be embedded in the organization's business continuity management practices.
	Compliance	Information should be protected to meet legal, statutory, regulatory, and contractual obligations and comply with the organization's policies and procedures.
Data Management	Human resource Security	Employees and contractors should be aware of their role in safeguarding the organization's information before and during employment. The organization's information should also be protected.
	Asset Management	Organizations should identify their physical and information assets and determine the appropriate level of protection necessary for each.
	Information security incident management	Information security incidents should be handled consistently and effectively.
Operation Security	Access Control	Access to information and information processing facilities should be limited to prevent unauthorized user access. Users should be responsible for safeguarding their authentication information, such as passwords.
	Cryptography	Policies on cryptography and the use of cryptographic keys should be developed and implemented to protect the confidentiality, integrity, and/or availability of information.
	Physical and environmental security	Controls should be introduced to prevent unauthorized physical access, damage, and interference to information processing facilities.

	Operation Security-	Procedures and responsibilities, Protection from malware, Backup, Logging and monitoring, Control of operational software, Technical vulnerability management and Information systems audit coordination
	Communication security	Information should be protected in networks and as it is transferred, both within the organization and externally.
	System acquisition, development and maintenance	Information security should be designed and implemented throughout information systems' lifecycle. Test data should also be protected.
Monitoring of suppliers	Supplier relationships	Any of the organization's information assets that are accessible by suppliers should be appropriately protected.

Source: contribution of the present research to the grouping above, based on ISO 27002 data

In addition to ISO 27002 certification, there is another strong driver when it comes to data protection, The EU General Data Protection Regulation (GDPR), which states that organizations must adopt certain policies, procedures and processes in order to protect the personal data they own (Lopes et al., 2019). Based on the concept of privacy as a fundamental human right, it has seven main privacy principles (fairness and lawfulness; purpose limitation; data minimization; accuracy; storage limitation; and integrity and confidentiality; accountability) and is considered one of the forerunners of uniform legislation regarding data security breaches (Tankard, 2016) and the most important change in data security in 20 years (Lopes et al., 2019). The GDPR imposes strict obligations on data processors, one of which is data breach notification, guarantees rights for data subjects, demands security and responsibility obligations, defends users' rights, such as the "right to be forgotten", establishes rules specific for email marketing and provide severe sanctions for companies that do not comply with the rules. For having great relevance, GDPR has impacts all over the world and is considered by many companies, even if they are not European, as a guide in terms of data protection, as will be shown later. In the US, the main data protection law is the California Consumer Privacy Act, CCPA, which became effective in January 2020. This Californian law provides several user rights, such as the right to delete personal information and opt-out of sales and is considered the law reference when it comes to the USA.

Up to now, both the GDPR, considered the legal driver that influences data protection not only in Europe but worldwide, the CCPA, one of the US references, and ISO 27002, a certification that establishes good practices that companies should follow, have been addressed so far. However, in order to have a broad understanding of the issue, it is necessary to know about the practical results obtained by companies and countries that take or do not take measures to protect their data. For this, this research will use the annual report of NSFOCUS, Inc., a global network that deals with cyber security and provides analytical insight into cyber-attacks.

From the points mentioned above, it is clear the importance of approaching the topic of data security and relating it to the value attributed to the consumer. In addition to being a current issue and one that has become more and more essential each year, it is an issue that inevitably affects the lives of all consumers. Because the capture and use of data has advantages and disadvantages described above, this paper seeks to understand the main practices that allows companies to stand out in terms of data protection. Considering the large impact of data management, this study aims to contribute to elucidate, applying the method presented below, which measures bring the most value to consumers.

3. METHOD

During the research, it was necessary to collect data and convert them into information; statistical techniques can assist this process. However, prior to analysis, the researcher must prepare their data in order to assess whether they are valid (Hair et al., 2005; Malhotra, 2001). The data needs to be revised, ensuring its integrity (Hair et al., 2005; Malhotra, 2001), process that has already been done by Just Capital, which made the manipulation check, observing whether there are missing data or signal failures in data collection and/or entry. Furthermore, there may be a need for the data to be transformed, which consists of modifying the collected data in a new format, for example, to combine categories (Hair et al., 2005; Malhotra, 2001). This method will be used in this research, so that it is possible to reach the desired results, as it is detailed further on.

This section discusses the methodological procedures used in this study, respecting the research strategies mentioned above. A quantitative methodology supported by Just Capital research from 2020 was used, which solicited input from both American public and subject matter experts, dividing the research into four steps: (1) Survey research, conducting a

representative sample of the American public, in order to understand the corporate behavior on public point of view and its relative importance and weight, (2) Company evaluation, which companies are evaluated trough Russell 1000 Index. After that, (3) Company data review, which companies have the opportunity to review data and (4) Ranking, when the classification is created and the industry-level ranking is available (Just Capital, 2020). Based on this survey, a group of variables is developed that aims to measure how companies deal with these issues based on each stakeholder that is affected the most by them. This is used to create company scores and ranks.

Just Capital's basis proves to be extremely valid for this research, as it provides rich information about many companies segmented by different variables and different weights for each. Among them, data privacy, which allowed the research to use this database as an important artifice, whose data have already been cleaned and verified. In addition, the companies verified in the base reside in one of the countries that most provoke and suffer from cyber-attacks in the world, EUA, which is deeply relevant for the research.

The database methodology procedures were consulted, and the information provided to establish what variables create value for each by the platform (JUST Capital, 2020), and grouped them as follows based on what is imperative for each stakeholder. The variables were compared with the overall weighted average score for each company. Also, after computing the scores, the results were analyzed in accordance with the previous literature, by looking at both theoretical and empirical papers that study value distribution among stakeholders. The results are clarified accordingly in the discussion section.

The Customers measures whether a company (1) protects the privacy of customers, including their data; (2) treats customers with respect and provides a positive customer experience; (3) makes products or offers services that do minimal harm to society; and (4) is transparent in communications about its products and services, beyond what is required by law. In this paper, the focus will be on the first one, so that it is possible to analyze the perceived value of the data privacy issue by the customers' point of view, considering some imperative variables that consumers appreciate, as service rating, transparency, honesty, privacy, data oversight, quality and product (JUST Capital, 2020; Olar&Jhunior, 2019).

Based on the methodology used by Olar (2019), this research took advantage of the metrics of data protection shared by Just Capital (2020) and, in order to be more assertive in this analysis, there were selected some of the principles of ISO 27002 to guide the research of

what supposed to be imperative on the data protection universe. Four principles stood out: confidentiality, integrity, authenticity and availability. The first concerns the exclusivity of access to certain data, ensuring secrecy and information security, while the second advocates that the stored data remain complete and resistant of failures. Authenticity is about the authorship of a given piece of data, through it is possible to guarantee that it was a certain individual who sent a piece of information. Lastly, Availability guarantees that information is available to everyone who needs it. Below, the metrics considered most relevant for this study, considering these principles (JUST Capital, 2020):

Table 1 - Metrics of Data Privacy from Just Capital database

Metrics	**Definitions**
Customer Data Selling	Is an assessment of whether the company states that it does not sell users' data, this metric was selected considering confidentiality and integrity principles
Tracking of User Activity	Is an assessment of whether the company explicitly states that it does not track users' behavior or complies with "do not track" requests. This metric was selected considering mainly the integrity principle.
User Control over Data Retention	Is an assessment of whether the company gives users full control over their own data. This metric was selected considering availability principles.
User Data Security Breaches	Is an assessment of whether the company clearly discloses its process for notifying users whose data might be affected by a data breach. This metric was selected considering integrity and confidentiality principles.
Data privacy controversies	Is the total number of cases occurring globally that pertain to privacy violations, as reported by influential and highly influential news sources over the past three years. This metric was selected as it exposes the importance of the data protection issue. This metric was selected considering integrity and confidentiality principles

Source: Table extracted from Just Capital database

Ideally, this research would run the metrics that most relate to the principles exposed above by ISO 27002. Nevertheless, the database that was granted access did not achieve this level of granularity of information. The scores from the metrics, instead, provides the consolidated result, represented by the variable CUST.PRIV, which is the grouping of variables CUST.PRIV.CONT and CUST.PRIV.MGMT. In order to clarify this segmentation of results, the grouping below was developed:

Table 2 - Gouping Variables of Just Capital

CUST.PRIV	CUST.PRIV.CONT	CUST.PRIV.CONT.PRIVACYVIO	-
		CUST.PRIV.GOV.OVERSIGHT	-
	CUST.PRIV.MGMT	CUST.PRIV.QUAL.CHANGES	CUST.PRIV.QUAL.CHANGESADV
			CUST.PRIV.QUAL.CHANGESDISC
		CUST.PRIV.QUAL.LANGUAGE	CUST.PRIV.QUAL.ENGLISH
			CUST.PRIV.QUAL.SPANISH
			CUST.PRIV.QUAL.OTHER
		CUST.PRIV.QUAL.POLICY	CUST.PRIV.QUAL.DISC
			CUST.PRIV.QUAL.EASE
		CUST.PRIV.UI.DATAUSE	CUST.PRIV.UI.ADVERT
			CUST.PRIV.UI.SELL
		CUST.PRIV.UI.TYPE	CUST.PRIV.UI.ONLYNECC
			CUST.PRIV.UI.DISC
		CUST.PRIV.UI.DATACONTROL	CUST.PRIV.UI.TRACKING
			CUST.PRIV.QUAL.POLICYSCOPE
			CUST.PRIV.SECURITY.BREACHES
			CUST.PRIV.SECURITY.NOTIFY
			CUST.PRIV.SECURITY.OVERSIGHT

Source: Table extracted from data provided by Just Capital database

The variable CUST.PRIV.CONT presented many constant results, which discouraged its consideration. In order to have a more assertive result, and without prejudice, only the variable CUST.PRIV.MGMT was used, in a context that all metrics mentioned above are included in this variable.

Taking this into account, the scores was computed in order to find associations and results in accordance with the previous literature, considering theoretical and empirical papers. In this process, in order to have an answer the closer to reality as possible, two relevant groups will be made for the study. The first one refers to the segmentation of companies in their respective industries, information that can be extracted from Just. The second of them refers to

the grouping of the 33 industries resulting from the grouping mentioned above into six main industries: Commerce; Manufacturing; Services; Utilities; Finance; Information Technology, following Boaventura et al (2020) classification:

Table 3 - Industry Grouping

Industries Grouping	**Industries**
Commerce	Commercial support services; household goods & apparel retail; food & drug retailers; personal products; food, beverage, & tobacco.
Manufacturing	Industrial goods; semiconductors & equipment; building materials & packing; automobiles & parts; chemicals; commercial vehicles & machinery; aerospace & defense; pharmaceuticals & biotech; oil & gas; basic resources
Services	Media; health care equipment & services; energy equipment & services; restaurants & leisure; real estate; health care providers; insurance; transportation
Utilities	Utilities; telecommunications
Finance	Capital markets; banks; consumer & diversified finance
Information Technology (IT)	Internet; computer services; software; technology hardware

Source: Table extracted from Boaventura et al (2020)

After getting the scores, the results are analyzed, along with the theoretical basis already mentioned, so that it is possible to establish relationships and connections between the industries, the metrics and its scores and the value concept. A ranking of the companies that

scored the most in the data privacy score used and the subsequent analysis of their public reports is fulfilled, to obtain practical results of the companies' actions.

For this, the 5 best-rated companies in each industry and their annual report for 2019 were ranked, considering the Investor Relations reports, which is available on the companies' website. It was understood that a more reliable result would be obtained when analyzing the reports of the same reference year of the Just Capital base, therefore, all reports refer to the year 2019, mitigating conclusive errors.

The 2019 reports were analyzed with a focus on the data privacy sector and the actions of companies regarding this matter. After observing data saturation contained in these reports, it was found that the qualitative analysis of 3 top companies from each industry would be enough to reach a satisfactory result for the research, as the actions were repeated in the other reports. After this step, the research consolidates the results into a single table, which brings together all the companies analyzed and which actions they most practice, according to the grouping indicated by Just Capital.

Therefore, this research aims to contribute to a topic that has its importance increasing as the use of data and related algorithms are widely used by companies. Since it is a subject that affects everyone who is minimally involved with technology, to answer the question of what are the best practices of data protection that create value for consumers generates great value to society, to companies, and to the academic literature, which will be able to further develop research.

4. RESULTS

The following results were collected in 2019 and published in 2020 of 922 companies listed on the US stock exchange. To determine the privacy value of the data from a consumer perspective, we analyzed the scores for the CUST.PRIV.MGMT variable, collecting the average, mode, variance, and standard deviation of the companies grouped into the six industries. Concomitantly with this analysis, we reduced the number of sectors to more assertively examine the data by industrial sector. After that, the companies that had the best results were qualitatively explored and then a comprehensive analysis of the context of the theme was inspected by NSFOCUS reports.

4.1. Quantitative Statistical Analysis of Just Capital

Focusing on the mean results of the CUST.PRIV.MGMT metric, the sector that holds the highest score is the Information Technology industry, with 68.71. This value is almost 7% higher than Finance, which ranks second in the results, with 63.71. When the other macro industries are observed, Commerce, Manufacturing, Services and Utilities have very similar results, between 43,62 and 47,25.

On the one hand, it is reasonable for companies that deal with technology to have more expressive results in terms of data security, as data is part of the core business and if there is no security in this regard, the reputation of the company is compromised. Finance companies, on the other hand, also have data security as a market requirement. Because they carry sensitive consumer data, such as bank details, financial routine and economic power, the responsibility for data security is manifest. In addition, as this segment of industry contains such important data, intrusion attempts are recurrent, which forces companies in this sector to evolve quickly in data security.

When other sectors are placed in the focus of the analysis, it is observed a great managerial opportunity especially for sectors that deal with the final consumer, such as Commerce and Services. Unlike the Information Technology and Finance industries, data security is not deeply tied to the core of these businesses. Despite this the evolution of data, especially after the COVID 19 pandemic, forced companies to use more than ever technological

and digital means in order to continue with their activities, in a context that face-to-face activities were being avoided as NSFOCUS report shows.

Mode result makes it explicit which score in each industry was most present in the Just Capital assessment. Below, it is possible to see that in this statistical measure the finance and information technology industries also have higher values than the others, following what was found in the above analysis. Furthermore, it is possible to infer that the commerce, manufacturing, services and utilities industries have the same most frequent score, 27.0557. Going deeper into this result, a significant number of companies performed with this result, a total of 114 companies, being the most repeated score among all. Understanding that this is not a significant result in terms of data protection, when the mean for each industry is put as a parameter, an additional analysis was performed. According to the histogram above, of 992 companies analyzed in the study, 48% have a score lower than 42, a result considered unsatisfactory for the analyzed variable, since the worst result among the industries was manufacturing, with 43.79 points. The histogram shows positive asymmetry, so that the mean of the distribution is greater than the median, that is, most of the data is below the mean.

If, on the one hand, Just Capital extracts results from many companies, different from each other, and which have distinct realities, on the other hand, the security and protection of user data is an extremely relevant topic and that it has been gaining strength every time most. Therefore, it is worrying that almost 50% of the companies analyzed have unsatisfactory results in a metric that can directly affect consumers.

When a database is ranked from the mean, this ranking is not necessarily accompanied by the median results, because the median translates the central value of the ordered data. Basing a result only on the mean, therefore, can lead to partially correct conclusions, as there may be some companies with very high scores, yet many with low scores, and even then, the mean will be pushed up. Below, the median follows the ranking of the mean in the two winning industries, finance, and information technology, with the services and commerce industry having the same median score. Therefore, the only change from the mean view would be for the manufacturing industry to score more than the utilities industry. This statistical metric was important for the research, to further reinforce and confirm the ranking object of research.

Conceptually, standard deviation is a measure that indicates the dispersion of data within a sample relative to the mean. In this work, the calculation of the standard deviation, together with the mean, aims to bring more content for the evaluation and differentiation of the behavior

of different industries in the data protection item. Table 4 below shows that the information technology and finance industries have higher standard deviation results, but the boxplot presents itself as a more visual tool of the results of this statistical metric. Thus, as the sample values are well distributed around the mean, we have a greater standard deviation. The opposite also happens, when the data are condensed around the mean, it means a standard deviation relatively smaller than the first option. For analysis purposes, the plotting of data from the industries was carried out jointly, so that in the same graph it is possible to compare the results of different industries.

As mentioned, the financial and technology industries have larger interquartile ranges than other industries, which, following the results in the table, have relatively close ranges. Furthermore, it is possible to infer that the Manufacturing, Commerce and Services industries, especially the latter two, demonstrate the presence of more outliers than the other industries, such behavior denotes a departure from a solid grouping that respects a representative data pattern. A possible explanation for this is the fact that these industries bring together companies from very different sectors, in the case of commerce, for example, we combine retail companies with food or beauty companies. In this case, they fall into the same sector, but it is understandable that they are at different times in the technological evolution related to data protection. In the case of finance, it is the opposite, because, although the standard deviation is one of the largest, the companies that make up this group are banks and companies related to the financial market, that is, their concerns and objectives are more aligned than the other industries, so we don't even see the presence of outliers.

Finally, the graph alerts us to a point of attention in the industrial manufacturing sector, which in addition to having the worst mean, still has a low level of standard deviation, showing consistency and homogeneity in the unsatisfactory result regarding data protection.

Based on the estimation of data protection value created and searching for the mean of the data from CUST.PRIV.MGMT, a rank was created looking for the enterprises that most

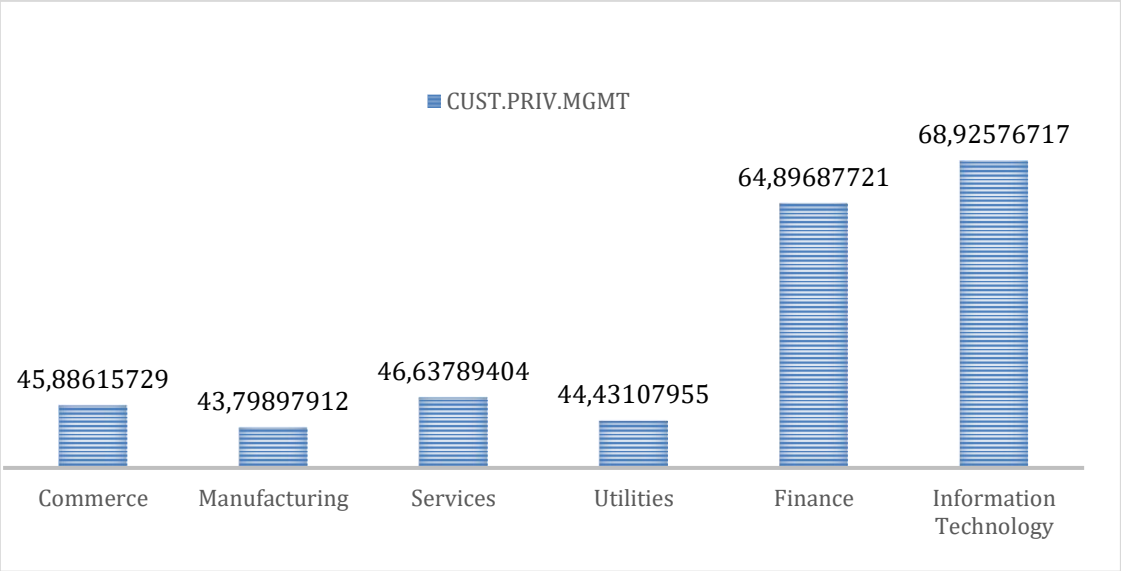
performed in which industry group. With this information, it was possible to verify in the public report of each one the importance given to the issue of data security.

Table 4 - CUST.PRIV.MGMT Results

Industries	**Mean**	**Mode**	**Median**	**Standard Deviation**
Commerce	45,886157	27,0557	41,0124	22,29064488
Manufacturing	43,798979	27,0557	39,46165	20,34272373
Services	46,637894	27,0557	41,0124	22,44725065
Utilities	44,43108	27,0557	36,360175	23,91051734
Finance	64,896877	36,360175	61,17205	27,97619214
Information Technology	68,925767	48,7661	62,7228	28,89146354

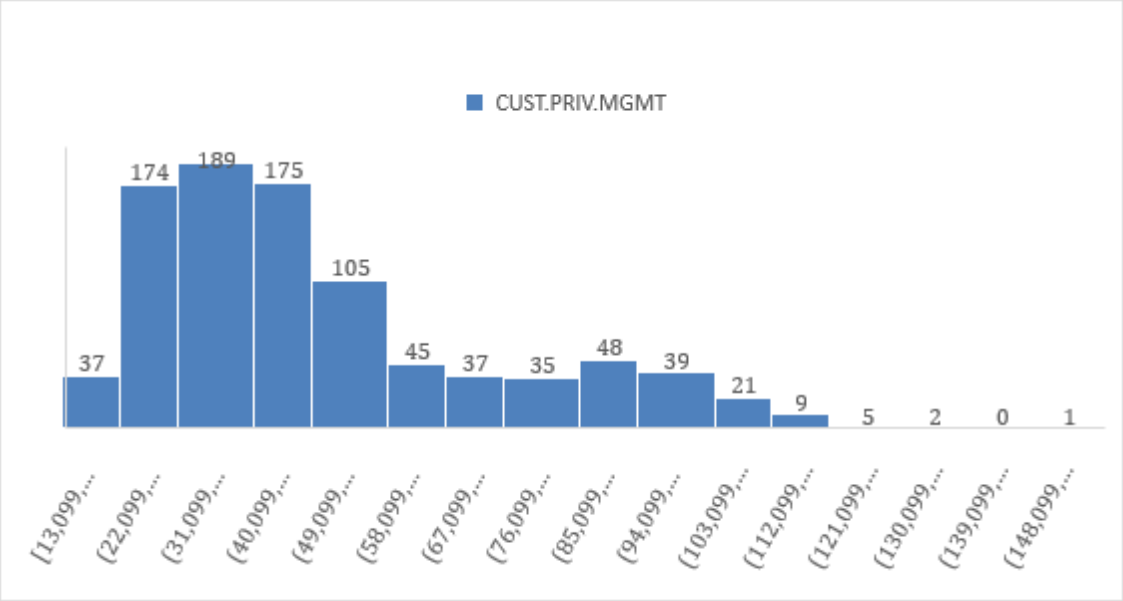
Source: Table extracted from data provided by Just Capital

Gráfico 1 - CUST.PRIV.MGMT Mean Results



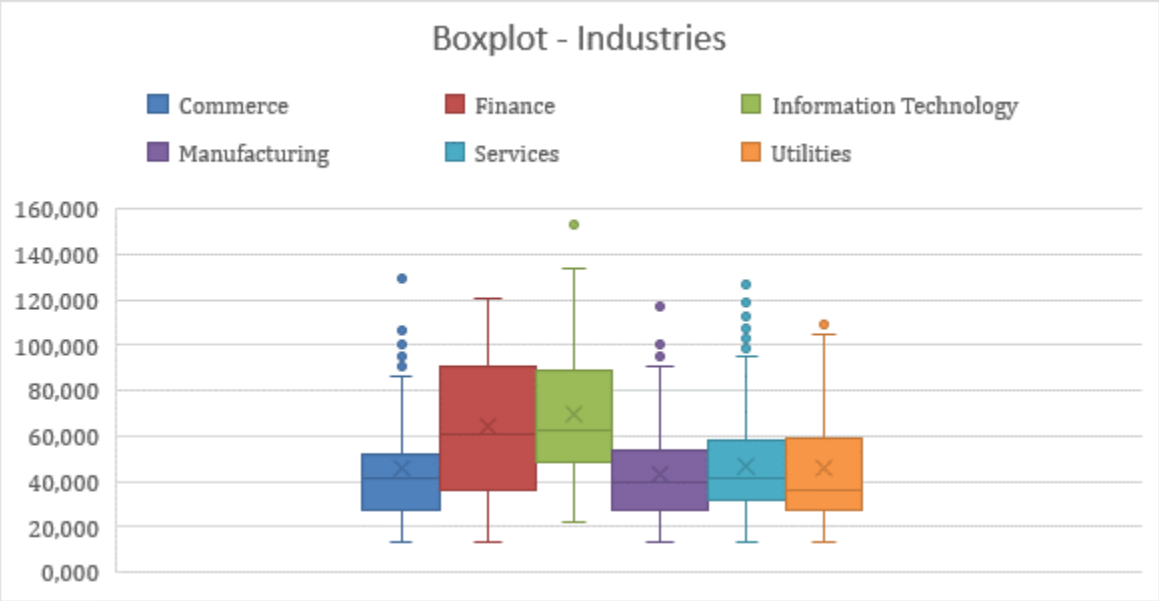
Source: Table extracted from data provided by Just Capital

Graphic 1 Histogram - CUST.PRIV.MGMT



Source: Table extracted from data provided by Just Capital

Graphic 2 - Boxplot Industries



Source: Table extracted from data provided by Just Capital

Table 5 - Five best companies in each industry in the variable CUST.PRIV.MGMT

Commerce	**Manufacturing**	**Services**	**Utilities**	**Finance**	**Information Technology**
Urban Outfitters Inc	Intel Corp	Nielsen Holdings PLC	AT&T Inc	PNC Financial Services Group Inc	Apple Inc
Etsy, Inc.	PRA Health Sciences, Inc.	Baxter International Inc	Sprint Corp	S&P Global Inc.	Akamai Technologies Inc
The Procter & Gamble Company	NVIDIA Corp	Anthem, Inc	Zayo Group Holdings, Inc.	IHS Markit Ltd	Microsoft Corporation
Paypal Holdings Inc	Celanese Corporation	AXA Equitable Life	Eversource Energy	Moody's Corp	Alphabet Inc

		Insurance Co			
Uber Technologies, Inc.	General Motors Company	Delta Air Lines Inc	T-Mobile US, Inc	The Western Union Company	Adobe Inc

Source: Table extracted from data provided by Just Capital

4.2. Qualitative Statistical Analysis

Below, the main actions and concerns of the 3 companies that performed the most in the CUST.PRIV.MGMT variable and disclosed their results in public annuals reports. The report analyzed is from 2019 and was collected on the companies' own website, as already detailed in the methodology section. The purpose of this section is to qualitatively understand and descriptively translate what are the actions of companies in favor of data protection, so that it is possible to relate this to the direction of iso 27002.

4.2.1. URBN – 2019

URBN cites GDPR and CCPA as regulations that have high potential to impact its maintenance of brand relevance and sales. This is because of the rules imposed by these regulations, which directly impact the rules of digital marketing. The company cites several risks that the company is subject to, when it comes to data security and, therefore, mentions some measures adopted that help to avoid problems in this regard:

Figure 2 - Actions taken by URBN to Protect Data

Implement systems and procedures designed to protect customer, employee, supplier, and company information
Prevent data loss and other security breaches

Identify, assess, and analyze cyber security risks
Carefully select your vendors

Source: URBN, 2019 annual report

4.2.2. ETSY – 2019

The report highlights the fact that there are several laws and regulations governing data security and that they are sometimes approached in different ways, which creates a complexity of application for international companies, which eventually need to adapt to different countries. Another challenge is that, even within the same country, there are regulations of different dimensions, such as consumer laws and payment processing laws, that dictate how electronic commerce should work and this complexity sometimes generates additional costs. In addition, according to the report, regulations affect the scope of the company, limiting its power to act in generating marketing ads and advertising in general. And, although the company strives to follow all the determinations, its performance in data security is limited, as it uses third-party services, which sometimes manage sensitive information and processes, such as payments. This becomes a risk, as Etsy has no way of controlling the security capacity of its partners and therefore failures can happen. Etsy is aware of regulations seen as international benchmarks, such as the GDPR and the CCPA, and their constant updates. Below, we list some of the main actions that the company is working to contribute to data privacy:

Figure 3 - Actions taken by ETSY to Protect Data

Establishment of Privacy Policies and documentation relating to the collection, processing, use and disclosure of personal data
Be aware of regulatory changes in the ways we and our suppliers collect, use, and share personal information.
Technical safeguards application

To have an intensive program of monitoring
To test constantly aspects of security internally and with outside vendors
To have an incident response program
To promote employee training programs

Source: ETSY, 2019 annual report

4.2.3. P&G – 2019

P&G sees potential security flaws and vulnerabilities that could lead to cyber intrusions as a major risk to its brand reputation. Some other risks linked to this failure are operational disruptions, impact on the supply chain, diminished brand power and reputation, compromised financial, business and personal data, as well as exposure to government regulations.

In order to mitigate such risks, the company maintains an information technology management that is reviewed by cross-functional technicians. In this program, an analysis of emerging cybersecurity threats is carried out, in order to outline plans and strategies to mitigate possible errors. The management of processing technologies, systems security and software is done on an outsourced basis, so that they are responsible for areas such as the collection, transfer, processing of data from all fronts involved in the business, respecting and following the guidelines of the regulations of the General Data Protection Regulation.

The evolution of cyber threats has proven to be a security risk for all services, systems, networks and supply chain. In order to face this movement, the company allocates investments that seek to resolve possible system vulnerabilities. Thus, they seek to monitor, update systems and networks, increase specialization in information security, train employees and constantly review the internal and supplier security policy. The company emphasizes that so far it has not

had any episode of cyber attack in its history, but that efforts to maintain this must be constant, which implies that system and technology updates are made on a recurring basis.

4.2.4. INTC - 2019

Intel understands solutions involving data as the driving force of the business, and for this it foresees solid foundations, with the development of a technological portfolio, making its practices and operations in its internal areas available to laws and regulations. It is in this context that concerns about breaches and data privacy requirements stand out. Although the correct action on this point is costly, we have that the negative impacts of negligence in the data privacy issue are even greater.

4.2.5. PRAH – 2019

PRAH is aware of regulatory requirements and trends that data privacy has placed on the corporate world. In this line, it carries out an inspection of the norms imposed by these regulations. Two of them are cited in his report as examples of data protection drivers, the GDPR and the CCPA, which have shown themselves to be trends to be followed in the world. One of the issues raised by the PRAH is the high value of the sanctions that non-compliance with these determinations entails in regions, to creating an obligation to expand mechanisms that ensure compliance with privacy laws. In addition, if you suffer from a cyber attack, your reputation could be affected and there could be unforeseen legal costs.

4.2.6. NVIDA – 2019

NVIDIA, as well as the other companies analyzed in this study, also uses confidential and personal data and sensitive information, and one of the company's biggest concerns is precisely related to the company's reputation linked to data protection. There is also fear about the laws and monetary sanctions that a possible incident could cause, in addition to the negative impact on the financial result, through security costs, regulatory procedures and increased legal costs. NVIDIA is aware of the movement in the data protection market, from GDPR, and stricter

laws also in the US, but its report brings a reactive tone, to the detriment of concrete preventive actions that avoid possible inconveniences.

4.2.7. NIELSEN – 2019

Nielsen is a global company that provides diverse visions and insights, also operating in the sphere of digital media, research market and audience analysis. Its objective is to bring data visibility to the business, as its core business is closely linked to data, which is sometimes sensitive. That is why your performance in data protection is so important and is directly related to your brand reputation and financial success. Approaching ETSY's vision, Nielsen also sees some data privacy regulations as harmful to its business, given that its way of operating comprises questions and consent to the provision of data by third parties. It is also important to emphasize that the company follows the trends of the others in this series of reports, to mention the GDPR, in Europe, and the CCPA, in the United States. It is possible to say that Nielsen fears the loss of control over its data, exposure to potential litigation, the compromise of its brand reputation, loss of trust on the part of its customers, being affected if a system intrusion occurs, loss of investments, financial sanctions and statutory penalties, in addition to the significant increase in cybersecurity costs.

4.2.8. BAX –2019

Baxter mentions data protection in its annual report and places the European data protection law, GDPR, as one of its main guides. In addition, it has a team of experts on the subject and provides training for its team. Another practice adopted related to this issue was the sharing of data protection clauses with its employees and its suppliers, also counting on online training that are available for access. The company understands the need for the rapid evolution of technologies while also following the acceleration of cyber attacks.

4.2.9. ANTM – 2019

Anthem understands that the company's success is linked to the level of trust it conveys. This premise is closely related to data protection, which is why the company dedicates some

practices in order to prevent cyber intrusions, such as: Hiring experienced professionals in the field of privacy and security with loads of leadership; Maintenance of a fast, multifunctional program in order to detect and assertively respond to suspected invasions; Monitoring, management and inspection of its programs and policies, based on current laws and regulations; Partnership and alignment between areas; Strengthen awareness of the topic, distributing pamphlets and educational messages to the teams, as well as promoting training and democratizing as control tools. In addition, it is worth noting that privacy corporate policies are updated annually, keeping a company always safe from data protection trends and recommendations. Its pillars of action in this regard include customer protection, concern with the technical safety of equipment, training, planning on privacy issues, regulatory alignment and internationally recognized certifications such as HITRUST. Below, some of the practical actions taken by the company, in the context of data privacy, according to the main pillars mentioned above:

Figure 4 - Actions Taken by PNC to Protect Data

Minimize the Attack Surface
Complicate Unauthorized Access
Rapidly Detect, Respond to, and Contain Potential Threats
Align Security Initiatives to Business Priorities
Maximize Operational Excellence

Source: ANTM, 2019 annual public report

1)

4.2.10. AT&T Inc – 2019

AT&T mentions in its report concerns about rising compliance costs, complaints against ISPs and increasing uncertainty in data availability and value, damages that can be exacerbated and intensified by cyber fragility. In this context, the report cites the data protection law in California, CCPA, which serves as a guide to overseeing the actions taken by the company. In addition, the report mentions that the trend of technological evolution brings the need for improvement in the use of software. This need is accompanied by the company's concern to have additional expenses with possible invasions in its system, which would generate negative impacts on the operation, on its brand reputation and on its financial condition.

4.2.11. SPRINT CORP – 2019

In Sprint Corp's annual report, a series of risks and uncertainties that impact the company's results are listed. Among them, we see concerns about the impact on the consumer's view of data privacy regulations. However, it is seen a report that does not guarantee that much emphasis, nor does it provide details on the operationalization of data privacy.

4.2.12. ZAYO – 2019

The company mentions the strict data privacy regulations used in both the US and the European Union, which especially include restrictions on the flow of data across borders, the General Data Protection Regulation and other data privacy requirements. Therefore, the company is concerned about the fact that these regulations are not made correctly, which could affect its operating and financial results.

4.2.13. PNC – 2020

Placed among the top three strategic priorities of the company, technological security is highly addressed in PNC’s 2019 report. The text states that the area that deals with cyber issues has received a high level of regulation, in addition to having a high impact on the generation of profit, and the technological evolution of payment systems should be looked at very carefully. One of the company's biggest concerns is having third-party services responsible for managing the infrastructure and system information. This is because the occurrence of any type of failure,

system interruption and information leakage can result in large losses to consumers and, consequently, the company would lose its credibility with them, which would impact its reputation and market share. By having under its control extremely sensitive information about its users, such as payment information, the company allocates a significant portion of its costs to the prevention and possible mitigation of the risks of failures and cyber attacks. The annual report for 2019 mentions that in recent years, several companies have suffered from data leakage, compromising the accounts and credentials of millions of users and this can even be a facilitator for invasions by malicious agents, who somehow already have some of these leaked data. Another loophole that attackers can find could be through users' personal devices, especially those that own financial applications. Understanding that attackers currently have many resources to carry out attacks and that in some cases it can even mean a limitation of action by the company, the PNC, to combat and prevent the high risks already mentioned, adopts some practical measures:

Figure 5 - Actions Taken by PNC to Protect Data

To have policies, procedures and systems designed to prevent or limit the effect of possible failures and breaches in security of information systems
To have devoted significant resources towards improving the reliability of our systems and their security against external and internal threats
To have information and technology risk programs to manage our capabilities to provide services in the case of adverse events that result into material disruptions.
To test the effectiveness of and enhance these policies, procedures, and systems.
Engage and monitor products or services provided by third parties that may generate risks and possible failures
To have a cybersecurity program that is designed to identify risks to confidential information, protect that information, detect threats and events, and maintain adequate response and recoverability to help ensure resilience against information security incidents.
To have training for all PNC employees and quarterly phishing exercises to raise employee awareness.

To be regularly examined by federal regulators

Source: PNC, 2019 annual report

4.2.14. SPGI – 2020

SPGI shows concern about investing in data security, it has invested in technology to consolidate data centers, applications to the cloud and strengthen cybersecurity. One of the operations that stands out in your report is precisely the reduction of cybersecurity risk, which should go hand in hand with the growth of the company's market brand. Within the forward-looking statements, the company demonstrates caution regarding the need to protect the security of confidential information and against unwanted interruptions.

4.2.15. INFO 2019

IHS Markit places data security and privacy within forward looking statements, addressing this issue with concern given the level of uncertainty, risk and hard-to-predict changes it carries. The impact on the company's reputation is one of the direct harms addressed, as the company deals with a wide range of sensitive and confidential information. Among the fears that the company has at this point are unauthorized access attempts, degradation of information, systems and networks, the introduction of malicious code and fraudulent "phishing" emails. Furthermore, threats are increasingly sophisticated, targeted and difficult to detect and prevent, which creates the constant need to take measures in relation to data protection, protecting it against vulnerabilities. That's because the consequence of a careless look can result in attacks and directly impact the trust of its consumers, corrupting its reputation and brand, in addition to being exposed to laws related to data privacy, which provide for fines and sanctions.

Among the company's actions to curb these damages are physical and technological security measures, control processes, contractual precautions with third parties, internal training, use of technology services from partner companies that help identify, protect and correct the information system. And, according to the report, not only do you need to take a cautious look at your own security measures, it is imperative to regulate and require your

subcontractors to maintain strict data security measures as well. And when it comes to projects that face many fronts within data information, such as the migration of new cloud-based solutions that the company has gone through, it is essential that there is a redoubled concern with the regulation of access security and with the prevention of network outages and possible failures, given that a time of transition like this can result in vulnerabilities and cyber attacks.

4.2.16. AAPL – 2019

The champion of the data protection metric score stamps its competitive advantages in the first pages of its annual report, and, among them, security is one of the main drivers of the company, alongside price, performance and quality. The fact that its market posture is subject to government laws and regulations is highlighted, which impacts the increase in responsibilities, as well as possible additional costs, aimed at mitigating possible risks. One of these regulations concerns data security and consumer protection, which is the focus of this research.

The report makes it clear that the reason for this concern lies in the fact that unauthorized access to or disclosure of confidential information, including personal identification, can negatively impact the company's reputation, both financially, legal and operationally. In addition, if this is not a point of attention, the company may suffer a data breach, which affects the confidentiality, integrity and availability of information, impairing the ability to retain customers, alienating potential suppliers, in addition to expose in front of government fines and sanctions.

As a way of acting on this topic, Apple dedicates significant resources to protecting its data network, also making use of encryption and other security measures used to protect data, such as authentication. In order to protect customers, Apple monitors its services looking for suspicious activity that could bring some kind of harm to the consumer. In addition, it guarantees substantial attention to the data security standards of the payment card industry, whose impact directly affects the company's reputation and reliability with its consumers.

4.2.17. MSFT – 2019

For Microsoft, expansion brings with it great responsibility and, with it, the expectation of earning and maintaining the trust of its consumers and partners. Trust is the foundation of the company's three pillars: privacy, cybersecurity and responsible AI. From the standpoint of privacy, the company defends it as a fundamental right and that, therefore, must be respected above all. Following this line, the company defends practices of transparency and storage responsibility. When it comes to cybersecurity, Microsoft benefits from a great data processing and authentication capability, also driving the innovative character of security.

Going deeper into the company's actions in these areas, we offer end-to-end security, covering a range of segments from identity to cloud applications and the infrastructure that this requires. In addition, the company establishes partnerships in both the public and private sectors, expanding this front, in the same way that it supports and follows the General Data Protection Regulation (GDPR) as a guide for its data privacy policies.

4.2.18. AKAM – 2019

If, on the one hand, the other companies in the analysis are afraid of encountering invaders, AKAM promises its customers precisely to deal with this problem. Having as its core business the creation of solutions for security, delivery and optimization on the internet, AKAM

It uses cloud security solutions, application protectors, interface and accessibility intelligence, which mitigates possible risks. One of its competitive advantages resides in its operations in different markets, ensuring the learning of patterns, vulnerabilities and visibility of traffic volume between different countries.

Like Microsoft, AKAM also highly values the trust its customers and partners have for its service, so it also values the reputation it carries, in terms of security.

In the report, we can still see the presence of important references in the field of data protection and security, such as the quotation from the GDPR, the California Consumer Privacy Act of 2018 and the CCPA. Based on these drivers, it is analyzed whether the actions taken favor the invasion of privacy or not. This is because if there are failures, the company's

reputation will suffer in front of the public, there will be reprisals before the law, inquiries from regulatory bodies, which should be vehemently avoided.

4.3 Qualitative Summary

Below, the consolidated view of the information showed above. It is important to emphasize the limitation of this table as being ok or not means only that the practice in question was not explicitly found in its public report, which means that companies that do not have the confirmation of the table may not clearly expose in the report, but, on the other hand, it is possible that the action was effectively accomplished.

Table 6 - Best Data Privacy Practices Found in Each Company

Pillars of Protection of Data	**URBN**	**ETSY**	**P&G**	**INTC**	**PRAH**	**NVDA**	**NLSN**	**BAX**	**ANTM**	**AT&T**	**Sprint**	**Zayo**	**PNC**	**SPGI**	**INFO**	**Apple**	**MSFT**	**AKAM**
Establishment of Privacy Policies and documentation	X	X	X		X	X	X	X	X	X		X	X		X		X	
Monitoring of suppliers	X		X						X				X		X			
Data Management		X	X				X	X	X				X		X			
Operation Security		X	X				X		X				X		X	X	X	

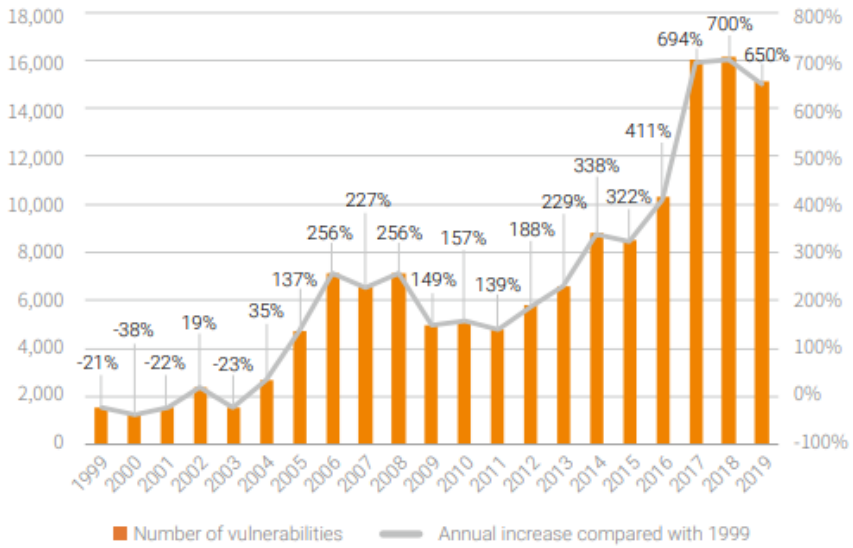
Source: Table extracted from public reports from 2019

4.4. Quantitative Analysis of NSFOCUS

From the published NSFOCUS report of 2019, the reference year for the study of this research, it is possible to understand the evolution of data breaches and, consequently, the increase in data protection by companies, making the battles increasingly intense. Regarding governments, there is a trend towards stricter law enforcement, which suggests a concern with proactive measures the report also addresses the growing use of mobile devices and how this also impacts the target of invasions. Below, some interesting insights will be presented that add to the understanding of the present research (NSFOCUS, 2019a)

In Figure 1, it is evident how the vulnerabilities evolved quickly. In other words, as the development of network technology and the rapid advancement of the internet in recent years has also caused the aggravation of cyber threats, due to the emergence of new systemic vulnerabilities. By the end of 2019, around 138,909 vulnerabilities were registered, whose annual increases are shown in the Figure below. It is noticed that the number of vulnerabilities has increased steadily and quickly since 2005 (NSFOCUS, 2019b):

Figure 1 - Number of Vulnerabilities

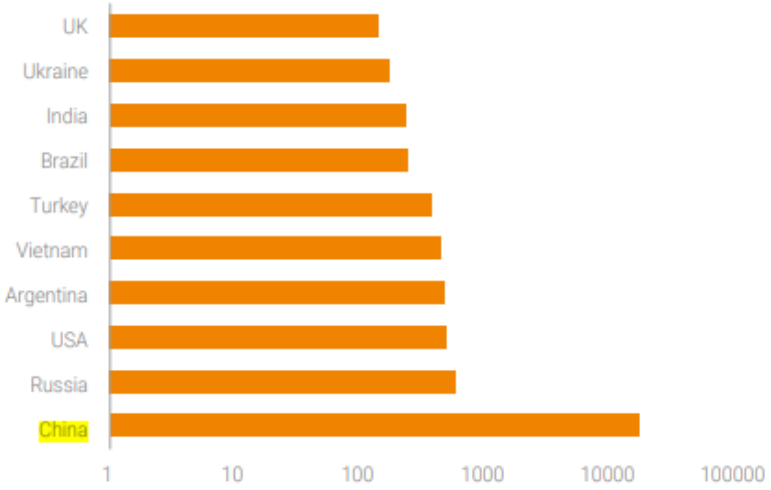


Source: NSFOCUS, Vulnerabilities and Threat Trends Research Report, 2019.

In geographic terms, according to the NSFOCUS report, represented by Figure 2, that shows the geographic distribution of cyber-attack sources; China had the highest proportion,

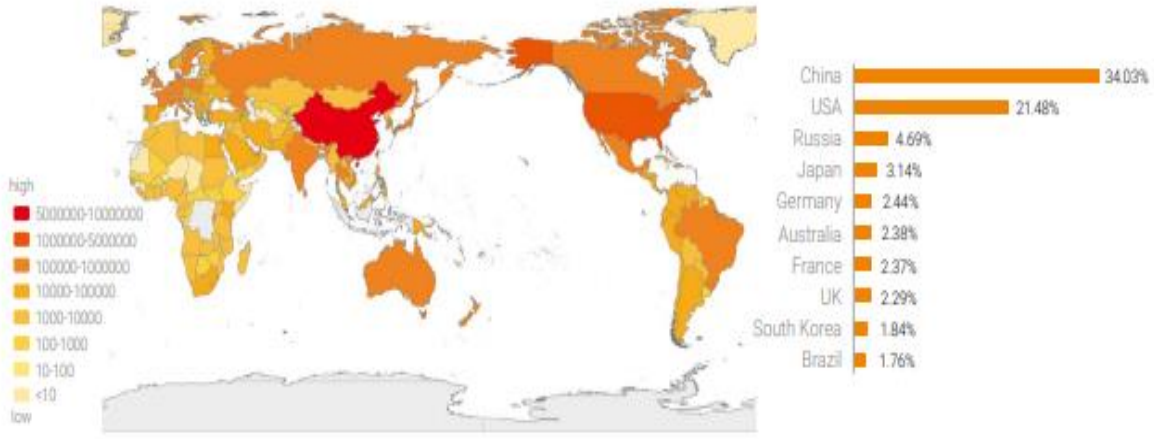
followed by Russia and USA. In the following figure 3, regarding cyber targets, China, the USA, Vietnam, India, and Brazil stand out as the main targets of attacks (NSFOCUS, 2019a). This view shows that, despite the US not being the best world reference for data security, it is still one of the countries that have more invading agents and the more targets found in the world. Therefore, research, focusing on a base of American companies, has the capacity to generate important insights.

Figure 2 - Global distribution of IP addresses of attack sources



Source: NSFOCUS, Cybersecurity Insights, 2019

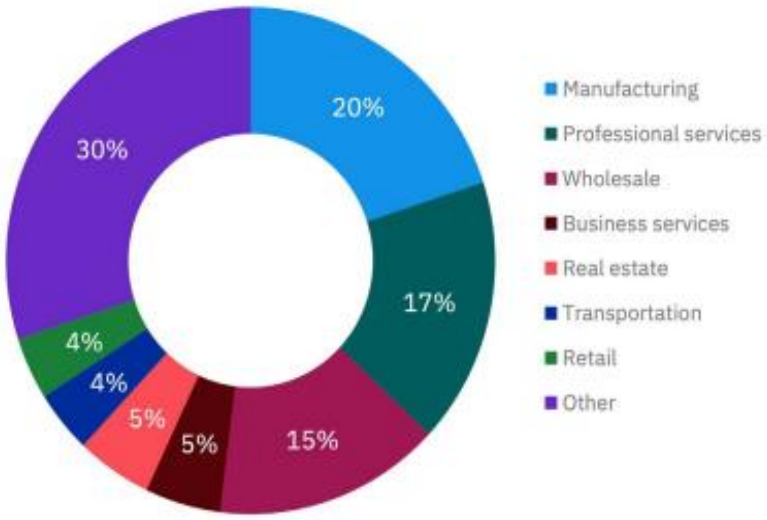
Figure 3 - Global Distribution of Source IP Addresses



Source: NSFOCUS, Cybersecurity Insights, 2019

When the industry is placed into the focus of the study, manufacturing, professional services and wholesale industries are the most impacted by malicious attackers, represented in the Figure 4 below. The analysis was made from the attacks provoked by the Sodinokibi, the most common ransomware type observed in 2020 by IBM Security X-Force. According to the NSFOCUS report, sometimes servers are not maintained properly, making attacks possible in sectors considered extremely profitable and capable of paying large amounts of ransom (NSFOCUS, 2019a).

Figure 4 - Percentage breakdown by industry of Sodinokibi ransomware attacks observed in 2020



Source: IBM Security X-Force

4.5. Management Contributions

From the data presented above, it is possible to draw important insights that can act as managerial contributions. When we look at the report of companies that stand out the most in data protection metrics, it is seen that many actions taken are repeated across companies. Most of them describe their practical actions to best protect your data and systems, some of which are listed below:

Figure 6 - Actions Taken by Companies for Data Protection

To follow regulatory polices taken as reference, such as the GDPR and the CCPA
To have authentication and encryption systems
Promote internal and external audits and inspections
Constantly seek improvements in data protection
To allocate teams focused on data protection
To train all the employees
To have risk management programs

Source: Public Reports from 2019, taken from the companies' website

In addition to the preventive, control and monitoring approach, some reports mention a reactive approach to damage. That is, sometimes, the company's effort to protect the data does not matter, since the invasion can happen by other means, for example, by suppliers, or even by an unknown technology, in which attackers have access, but the company does not. This shows the rapid evolution that information technology has advanced and how companies eventually also find themselves vulnerable and exposed.

The research also contributes to the understanding of which factors drive companies to acquire satisfactory data security. Below are those that appear in the reports:

Figure 7 - What Companies Consider Risks Related to Non-Protection of Data

Government fines and financial sanctions
Loss of brand reputation
Loss of consumer confidence
increase of operating costs caused by the mitigation of damage suffered

Source: Public Reports from 2019, taken from the companies' website

Lastly, it is interesting to note that not all companies have a positive look into the strict regulations based on data protection. That is because the protection of users' cyber rights reduces the effectiveness of some advertising actions, which, according to these companies, generates a reduction in profit, as they no longer have the space they had in communication and use of their users' data.

5. FINAL CONSIDERATIONS

In a context where data is considered one of the greatest assets in the corporate world, we are witnessing the acceleration of cyberattack attempts, which ultimately affect businesses and consumers. In this sense, this work was guided by a deeper understanding of the best practices related to data protection that generate value to consumers, based on Just Capital's 2020 database and considering the approach on value perception understood by the existence of safety, accessibility, business reputation and respect with consumers, specifically regarding data protection.

To reach this understanding, first the companies were segmented into six main industries, which had their scores analyzed, so that it was possible to obtain insights about the behavior of each one of them. After this step, a ranking of the companies that obtained the best results in the data protection variable was carried out and an analysis of their annual report was carried out, extracting the main relevant points that the company adopts to contribute to the protection of its data.

The research showed that the finance and information technology industries stand out in data protection and that, looking at the 18 companies that had their reports analyzed, some

practices performed among them are repeated. Among them, the importance given to regulatory polices taken as reference, such as the GDPR and the CCPA, to have authentication and encryption systems, to carry out constant audits, including their own suppliers, to have training and managerial positions dedicated exclusively to data protection, constantly look for technological evolutions in this direction, finally, monitor, control and act quickly in cases of cyber intrusion.

This study also allowed us to understand some opportunities for improvement in some sectors such as commerce, services and manufacturing, bringing important managerial contributions to the corporate environment. The main one refers to the verification of the best practices adopted by companies that are concerned with data protection and do not hesitate to place this aspect as one of the pillars of their management. This study was also important to understand patterns that lead to managerial decisions, such as companies' fear of suffering financial sanctions and losing their brand reputation, in cases where data is leaked. Another contribution was the categorization of data protection metrics in the Just Capital database, which could serve as an important instrument for future research that wants to go deeper into the subject.

Regarding limitations, the research uses only the 2020 basis of Just, not examining, therefore, possible evolutions in the metrics of companies with previous or more recent data. In addition, access to the metrics by the basis of Just Capital was not possible and no comparisons were made between the practices adopted by companies from other regions of the world, which could provide a more comprehensive view of the issue. Another limitation was having explored the data protection study focusing only on the eyes of consumers, and for future studies, it would be interesting to understand the perception of value of other stakeholders on the topic, such as shareholders, workers, government, among other agents. In addition, it is possible to carry out comparative studies with the most recent Just Capital database, compare the effects that the pandemic has brought to data protection, and understand what are the practices that destroy value, it would also be relevant conduct a research relating data protection with financial performance of the companies.

REFERENCES

1. Barocas, S., & Nissenbaum, H. (2014). Big data's end run around procedural privacy protections. *Communications ofthe ACM*, *57*(11), 31–33. https://doi.org/10.1145/2668897
2. Boaventura, J. M. G., Bosse, D. A., Manuela Cunha de Mascena, K., &Sarturi, G. (2020). Value distribution to stakeholders: The influence of stakeholder power and strategic importance in public firms. *Long Range Planning*, *53*(2), 101883. https://doi.org/10.1016/j.lrp.2019.05.003
3. Boaventura, J. M. G., Cardoso, F. R., da Silva, E. S., & da Silva, R. S. (2009). Teoria dos Stakeholders e Teoria da Firma: Un estudo sobre a hierarquização das funções-objetivo em empresas brasileiras. *Revista Brasileira de Gestao de Negocios*, *11*(32), 289–307. https://doi.org/10.7819/rbgn.v11i32.378
4. Chaorasiya, V., & Shrivastava, A. (2014). *and technologies: A survey on Big Data*. *275*(1), 314–347.
5. Donaldson, T., & Preston, L. E. (1995). The Stakeholder Theory of The Corporation: Concepts, Evidence, And Implications and from the specific comments of many people, including Professors Aupperle. *Academy of Management Review*, *20*(1), 65–91.
6. Freeman, R. E. (1984). Strategic management: A stakeholder approach. In *Strategic Management: A Stakeholder Approach*. https://doi.org/10.1017/CBO9781139192675
7. Freeman, R. E. (2011). Managing for Stakeholders. *SSRN Electronic Journal*, 1–22. https://doi.org/10.2139/ssrn.1186402
8. Günther, W. A., RezazadeMehrizi, M. H., Huysman, M., & Feldberg, F. (2017). Debating big data: A literature review on realizing value from big data. *Journal of Strategic Information Systems*, *26*(3), 191–209. https://doi.org/10.1016/j.jsis.2017.07.003
9. Harrison, J. S., Bosse, D. A., & Phillips, R. A. (2010). Managing for Stakeholders, Stakeholder Utility Functions, and Competitive Advantage. *Business*, *1154*(March), 1–43. https://doi.org/10.1002/smj
10. Harrison, J. S., & Wicks, A. C. (2013). Stakeholder Theory, Value, and Firm Performance. *Business Ethics Quarterly*, *23*(1), 97–124. https://doi.org/10.5840/beq20132314
11. JUST Capital. (2020). *Amidst Crisis, What Americans Want From Corporate America*. *October*. Retrieved from:

https://accounts.justcapital.com/download?file=8e34607577671197b1205f745d0ab170

12. Madsen, A. K. (2015). Between technical features and analytic capabilities: Charting a relational affordance space for digital social analytics. *Big Data and Society*, *2*(1), 1–15. https://doi.org/10.1177/2053951714568727

13. Meriah, I., &Rabai, L. B. A. (2019). Comparative study of ontologies based iso 27000 series security standards. *Procedia Computer Science*, *160*, 85–92. https://doi.org/10.1016/j.procs.2019.09.447

14. Olar, A. I., &Jhunior, R. de O. S. (2019). VALUE DISTRIBUTION TO STAKEHOLDERS: EVIDENCE FROM THE UNITED STATES. *The Bottom Line Manuscript*.

15. Orbik, Z., &Zozul'aková, V. (2019). Corporate Social and Digital Responsibility. *Management Systems in Production Engineering*, *27*(2), 79–83. https://doi.org/10.1515/mspe-2019-0013

16. Parmar, B. L., Freeman, R. E., Harrison, J. S., Wicks, A. C., Purnell, L., Bidhan, L., Edward, R., Jeffrey, S., & Andrew, C. (2010). The Academy of Management Annals Stakeholder Theory: The State-of-the-Art Stakeholder Theory: The State of the Art. *Management*, *936836193*, 403–445.

17. Priem, R. L. (2007). A consumer perspective on value creation. *Academy of Management Review*, *32*(1), 219–235. https://doi.org/10.5465/AMR.2007.23464055

18. Soares, C. S., Sarturi, G., & Boaventura, J. M. G. (2014). Afinal, o que é distribuir valor para os stakeholders? *Engema*, 17.

19. Solove, D. J. (2013). Introduction: Privacy self-management and the consent dilemma. *Harvard Law Review*, *126*(7), 1880–1903.

20. Someh, I., Davern, M., Breidbach, C. F., & Shanks, G. (2019). Ethical issues in big data analytics: A stakeholder perspective. *Communications of the Association for Information Systems*, *44*(1), 718–747. https://doi.org/10.17705/1CAIS.04434

21. Wigan, M. R., & Clarke, R. (2013). Big data's big unintended consequences. *Computer*, *46*(6), 46–53. https://doi.org/10.1109/MC.2013.195

22. ISO/IEC. (2013). ISO/IEC 27002:2013.pdf. *Iec*, *2013*, 90. www.iso.org

23. Lopes, I. M., Guarda, T., & Oliveira, P. (2019). How ISO 27001 Can Help Achieve GDPR Compliance. *Iberian Conference on Information Systems and Technologies, CISTI*, *2019-June*(June), 1–6. https://doi.org/10.23919/CISTI.2019.8760937

24. NSFOCUS, I. (2019a). Cybersecurity insights. In *InTech* (Vol. 66, Issue 2).

25. NSFOCUS, I. (2019b). *Vulnerability And Threat Trends Research Report 1day*.

26. Tankard, C. (2016). What the GDPR means for businesses. *Network Security*, *2016*(6), 5–8. https://doi.org/10.1016/S1353-4858(16)30056-3

27. Privacy & Security Standards - Anthem Company :: Anthem (anthemcorporateresponsibility.com)

28.