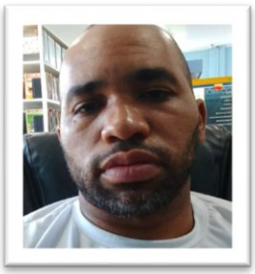
ISSN 1678-765X doi 10.20396/rdbci.v21i00.8671505/32354

Article

RDBCI
Revista Digital de Biblioteconomia e Ciência da Informação
Digital Journal of Library and Information Science

Surveillance of information flow and privacy in the digital environment

Arnaldo Luis Darg Moreira [1] Edelvino Razzolini FIlho[2]
Milton Cesar Adrião [3]



ABSTRACT

Introduction: The growing offer of products and services in a virtual environment resulted in a significant increase in the volume of personal and organizational data that transit through data networks and are stored in different places, by different entities. Interactions in this environment are continuously monitored, whether for needs related to the interests of companies or organizations, or to curb the most diverse illicit practices. These monitoring activities, which configure a state of permanent vigilance, raise concerns related to the treatment of data collected and processed, with important ethical and legal implications, and which may not be properly covered by legal instruments. Objective: The research sought to identify which studies published between 2010 and 2020 deal with ethical or legal issues related to privacy in the virtual environment. Methodology: A literature review was carried out, adopting content analysis as a technique. As a technological resource, Excel® and ATLAS.TI® software were used. Results: Only 19 of the 39 documents found are in line with the research objective, most of which are theses and dissertations. Publications are concentrated in the second half of the analyzed period. Conclusion: The analyses showed a growing need to monitor the information circulating in the virtual environment, involving sender and receiver, covering security issues, increased volume of data, new technologies, and cybercrime among other issues. The number and distribution of articles over the analyzed period indicate that these themes require even greater investigations, contemplating broader perspectives of monitoring activities in virtual environments.

KEYWORDS

Information. Ethics in information. Right to privacy. Social media. Information society.

Authors' correspondence

[1] Universidade Federal do Paraná
Curitiba, PR - Brazil
arnaldodarg@outlook.com

[2] Universidade Federal do Paraná
Curitiba, PR - Brazil
razzolini@razzolini.adm.br

[3] Universidade Federal do Paraná
Curitiba, PR - Brazil
milton.adrião@ufpr.br

Vigilância e privacidade no ambiente digital

RESUMO

Introdução: A crescente oferta de produtos e serviços em ambiente virtual resultaram em significativo aumento do volume dos dados pessoais e organizacionais que transitam por redes de dados e são armazenados em diferentes locais, por diferentes entidades. As interações neste ambiente são monitoradas continuamente, seja por necessidades relacionadas a interesses de empresas ou organizações, seja para coibir práticas ilícitas as mais diversas. Estas atividades de monitoração, que configuram um estado de permanente vigilância, suscitam preocupações relacionadas com o tratamento dos dados coletados e processados, com importantes implicações éticas e legais, e que podem não estar devidamente cobertas pelos instrumentos legais.

Objetivo: A pesquisa procurou identificar que os estudos publicados entre 2010 e 2020 tratam de questões éticas ou legais relacionadas com a privacidade no ambiente virtual. Metodologia: Foi realizada uma revisão da literatura, adotando como técnica a análise de conteúdo. Como recurso tecnológico foi utilizado o software Excel® e o ATLAS.TI®. Resultados: Apenas 19 dos 39 documentos encontrados estão alinhados com o objetivo da pesquisa, a maioria dos quais teses e dissertações. As publicações estão concentradas na segunda metade do período analisado. Conclusão: as análises evidenciaram uma crescente necessidade em monitorar as informações que circulam no ambiente virtual, envolvendo emissor e receptor, abarcando questões de segurança, aumento do volume de dados, novas tecnologias, crimes cibernéticos entre outras questões. A quantidade e a distribuição dos artigos ao longo do período analisado indicam que estes temas demandam ainda maiores investigações, contemplando perspectivas mais abrangentes das atividades de monitoração em ambientes virtuais.

PALAVRAS-CHAVE
Informação. Ética na informação. Direito à privacidade. Redes sociais. Sociedade da informação.

CRediT

- Acknowledgments: Not applicable.
- Funding: This study was funded by the Brazilian agencies National Council for Scientific and Technological Development (CNPq) for the scholarships and financial support granted. This study was partially funded by the Coordination for the Improvement of Higher Education Personnel - Brazil (CAPES), Financial Code 001.]
- Conflicts of interest: The authors certify that they have no commercial or associative interest that represents a conflict of interest in relation to the manuscript.
- Ethical approval: Not applicable.
- Availability of data and material: Not applicable.
- Authors' contributions: Conceptualization, Data Curation, Formal Analysis, Funding Acquisition, Research, Methodology, Project Management, Resources, Software, Supervision, Validation, Visualization, Writing – original draft, Writing – revision & editing: MOREIRA, A. L.D.; RAZZOLINI SON, E.; ADRION, M. C.
- Translation: Silvia Iacovacci - MEI

JITA: EH. Ethics in information and publications.

Article submitted to the similarity system

Submitted: 22/11/2022 – **Accepted**: 17/07/2023 – **Published**: 12/08/2023

Editor: Gildenir Carolino Santos

1 INTRODUCTION

For Choo (2003) information is an essential element for human activities, whether they are personal or part of organizational processes. The performance of activities often implies the need for information to guide these same activities. Information is thus an important input for human beings. Both Santos et al. (2021) and Silva and Razzolini Filho (2020) highlight the role that information plays in the decision-making processes of organizations, in their various scenarios.

Social and technological development has made the role of information as an enabler of human action more evident. In this era known as the information society, different technological resources are used for storage and transmission of data and information. Information-based innovations occur constantly, profoundly transforming the life of society (Assmann, 2000), inducing changes in informational behavior that, according to Carandina (2021), do not occur only through technological resources, but by the way these resources are incorporated into social practices. A space of interaction is configured on the technical infrastructure of the Internet, which allows different people, using different resources, such as computers, Smartphones, Smart TVs, among other devices, to interact in a virtual environment. In these environments, personal interactions and business transactions take place, which both depend on a flow of information that supports them and generate a flow of information to guide and record their activities and results. This information, whether in flow or stored on devices, is a valuable asset and this leads to the emergence of unethical or criminal activities in these environments, such as hacker attacks, which can invade systems and access information from public and private organizations (Canongia; Mandarino Junior, 2010), or the scandal that occurred in the National Security Agency (NSA) of the United States, where the government exceeded ethical limits in the collection of information (Van Dijck, 2017). The line between monitoring and espionage can be blurred. Thus, monitoring and surveillance activities, adopted as a way to prevent or combat crimes in these environments, can also be vehicles for illicit or unethical actions.

The monitoring of information flows in digital environments has been a matter of concern due to issues related to user privacy and the destination of information, which is collected as activities are carried out. There is a tension between the need to monitor these environments, to meet the needs and interests of the companies that maintain these services or the people and companies that participate in them, and the need to protect the participants of these environments, preventing indiscriminate access to information concerning them (Canongia; Mandarino Junior, 2010). Some of these participants may be involved in illegal activities on these platforms, and it is important to identify them and curb these activities (BALL; WEBSTER, 2003). The possibility of illegal acts leads to pressure for more effective and pervasive monitoring and surveillance mechanisms, which can adversely affect the right to privacy and produce harm to those affected (Ball; Webster, 2003; Henchke, 2017). Ball and Webster (2003), in particular, drew attention to the extent of surveillance mechanisms in modern society. According to them, surveillance, increasingly incorporated into everyday life by the action of state and supra-state agencies and corporations, is now routine, being a distinctive feature of modernity. It has, however, been largely underestimated in social analysis.

Twenty years on from Ball and Webster's (2003) work, the development of new technologies, new service and business models and the enactment of new regulatory frameworks may have rendered their considerations dated. It is therefore worth investigating what recent work has addressed these issues. Thus, the objective of the article is to identify which studies published between 2010 and 2020 have an intersection with information monitoring in the virtual environment. The article consists of five sections: (i) this introduction; (ii) theoretical foundation; (iii) methodology; (iv) results; and (v) final considerations.

2 THEORETICAL FRAMEWORK

The rationale is anchored by elements drawn from Ball and Webster's (2003) book on the challenge of privacy and the value of information. These elements are information monitoring and surveillance, information and virtual identities and, finally, ethics and legislation in the information monitoring process, as follows.

2.1 Monitoring and surveillance in the digital environment

Information monitoring is a very important procedure, helping organizations to meet their objectives. To this end, information needs to be monitored in different perspectives, involving: a) political element; b) economic element; c) technological element; d) environmental element; e) legal element; f) informational element. Monitoring the different scenarios in which information circulates avoids unnecessary risks, whether in simple decisions of an individual's daily life, or in decisions of the organizational environment that have greater complexity (Razzolini Filho, 2020).

Still for Razzolini Filho (2020), with the new technological resources and the varied forms of interaction provided by them, there is an excess of information circulating in different environments. New technological resources and changes in people's behavior regarding the use of such resources have continuously increased the number of individuals and the circulation of information in virtual communities, and actions in this environment, even if not illegal, can affect organizations. Thus, it is understandable that monitoring processes exist to promote or protect the interests of organizations, and it is important for them to monitor the information flow generated in the virtual environment, seeking new competitiveness strategies (Hoffmann, 2011).

From a governmental perspective, there is the issue of crimes that can occur in this environment due to vulnerabilities in equipment and networks (Damião, 2018) or illicit practices in these environments, such as racism, hate speech, pedophilia, information theft and even the creation of communities for crime planning. These concerns have also led to the practice of monitoring the information circulating in this environment, in which a user may be a victim or perpetrator of an offense (Lima, 2020). The in-depth investigation of these and other forms of cybercrime also requires monitoring mechanisms, which run into some difficulties. One of them is precisely the continuous change in the technologies used, which make investigative processes difficult, since they end up running into legal issues that have not followed this evolution (Goulart, 2021). Some techniques used in investigative processes have helped in solving cybercrime. An example is the case of the police officer who works undercover when using a fake profile (Goulart, 2021). However, this procedure raises a very relevant point about the user who, when using cyberspace, can assume any identity.

That is, there are legitimate monitoring processes maintained by organizations to protect their interests in the virtual world, there are monitoring processes maintained by platform owners to prevent and/or curb potentially illicit activities and there are investigation activities in the virtual environment, when illicit activities are already sufficiently characterized to allow action by security agencies. All these forms of monitoring, which aim to protect people and/or organizations, may affect individual rights.

This tension has not been ignored by academia. Ball and Webster (2003), for example, had already addressed it. Surveillance, for them, involves the observation, recording and categorization of information about people, processes and institutions. The process of surveillance, which we consider here to be equivalent to monitoring, requires capturing, storing, examining and transmitting it.

According to these authors, even though surveillance is a distinctive feature of modernity, increasingly incorporated into everyday life by the actions of state and supra-state

agencies and corporations, it has been largely underestimated in social analysis. Surveillance is now routine - it is hard to conceive of an activity today that is not producing data used in ways that escape the comprehension of those involved. People are surveilled when making phone calls, accessing the Internet, interacting with apps, making purchases, traveling streets or roads monitored by security cameras capable of image recognition to identify people and/or vehicles, paying tolls.

The mere fact of carrying cell phones enables surveillance processes. Surveillance, once thought of as monitoring or intercepting the actions of enemies, is now routine and ubiquitous and is even a central element in the most diverse strategies, whether subsidizing sales campaigns or directing political campaigns, to name just two examples. Thus, it is permissible to consider that surveillance, in the terms put forward by Ball and Webster (2003), which involves not only the collection of data, but its classification, generating categories that classify people according to the most varied criteria, is an inseparable part of organizational action, not only for the prevention of illicit acts. Classification is not an ethically neutral operation. It produces virtual identities that have important effects, as noted by Henschke (2017).

2.2 Information and virtual identities

Information has gained increasing importance over the years, especially in the organizational context, where the complexity of processes increases, leading to the need for new information in organizational procedures (Freitas *et al*., 1997). Barreto (1994) points out that the production of information has gradually increased according to the movements that have occurred throughout history, such as the industrial revolutions, which made it possible to implement new technologies in the process of storing, processing and disseminating the data obtained. In the hyperconnected world of the information society, information is the business.

It should be considered, however, that information is related to the perception and context in which data are presented, because while a given sign is just a data, for another person it can be information (Capurro; Hjorland, 2007; Razzolini Filho, 2020). Also for Ball and Webster (2003) data can have different meanings, and the context in which they are analyzed will influence the value and meaning that will be attributed to them. Surveillance processes involve the categorization of data, which is a way of assigning meaning to them.

This theme is also the subject of considerations by Henschke (2017), who draws attention to the fact that surveillance technologies provide particular epistemic actions, linking information to people, so that a person is the source of information, but is also the target of information. Surveillance technologies produce meaningful information about people, create identity relations between people in the world and the informational representation of these people produced by the processes of information aggregation. These virtual identities, as Henschke (2017) calls them, not only change the utility of information, but also alter the moral importance of this information.

It is relevant to highlight the effect of changes in the communication process, which migrated from a physical to a virtual environment, on the identification process, as pointed out by Malveira (2011). New technologies allow the same person to participate in the virtual environment, only needing to connect to social networking platforms, where they can even assume different identities. Their actions in these virtual environments, by the mechanisms presented by Henschke (2017), produce yet other virtual identities, these independent of any decision of these people. These virtual identities are embodied in data and information, collected and produced. The custody and protection of this information is also an object of attention. Both Ball and Webster (2003) and Henschke (2017) consider that, although there is a law on the privacy of information of service users, it is necessary to think about what destination organizations give to the data collected on different platforms. There is also the fact

that there are gaps in legal systems, leaving users potentially vulnerable.

2.3 Ethics and legislation in information monitoring

When addressing information monitoring, it is necessary to consider the ethical issue, as this procedure potentially involves the data of millions of people. According to Lévy (2008) cyberspace is the result of the worldwide interconnection of computers, and an ocean of information is fed by different people who navigate this environment. As they browse and interact, they leave records, in the form of clicks, views, posts, comments, transactions, shares and others. This data has been analysed by different organizations for various purposes, including understanding consumption patterns, identifying user profiles, recommending products, influencing people's behaviour towards products, services, organizations, candidates in elections or plebiscites, to name a few. But existing technologies capture not only data when making a purchase, filling out online forms or posting on social networks.

There are thousands of cameras responsible for the visual identification of an individual (Cella; Rosa, 2013). This data can also be used to monitor suspicious activities or individuals suspected of involvement in illicit activities. In doing so, they end up producing virtual identities, as expressed by Henschke (2017). Surveillance produces representations about people, which can have effects on them.

There is an ethical issue here, involving the principles and values that govern the conduct of people or groups who, by their conduct, participate in these processes (Cortella, 2017). There are also legal issues. Legal regulations have been adopted in several countries to ensure data protection and user privacy (Caldeira; Sarlet, 2019). In Brazil, the Brazilian General Data Protection Law, Law No. 13,709, of August 14, 2018 (BRASIL, 2018), known as LGPD, sought to provide citizens with greater control of their data, as well as regulate the use of information in businesses that use personal data in automated decisions (Monteiro, 2018).

This law was soon modified by Law 13.853/19 (Brasil, 2019). The principles of the LGPD, presented in the second article of this law, are respect for privacy; informational self-determination; freedom of expression, information, communication and opinion; the inviolability of intimacy, honor and image; economic and technological development and innovation; free enterprise, free competition and consumer protection; and human rights, the free development of personality, dignity and the exercise of citizenship by natural persons.

Article 4(III), however, states that the law does not apply to the processing of personal data carried out for the exclusive purposes of public security, national defense, State security or activities for the investigation and prosecution of criminal offenses, as well as to data from countries with similar legislation, provided that they are not shared with local agents. Exceptions to the law must be the subject of specific legislation, which must guarantee the fulfillment of the public interest in these cases, observing the principles of protection and individual rights provided for in this law (Brasil, 2018).

It should be noted that the LGPD encountered challenges when implemented, requiring both the adequacy of organizations, in the form of investments in systems and training of employees, and the effective performance of inspection activities by the responsible entities (Melo Cunha, 2021). The specific legislation mentioned in the LGPD has not yet been established, which makes the discussion on these issues even more relevant.

There is, in the Chamber of Deputies, Bill 1515/2022 (Brasil, 2022), which recognizes the legal gap that still exists in Brazil and proposes to establish a Personal Data Protection Law for the exclusive purposes of State security, national defense, public security, and investigation and prosecution of criminal offenses. This bill was the object of analysis by IRIS - Institute for Reference on Internet and Society.

The Technical Note issued (Azevedo *et al.*, 2022) recommends the filing of this bill, considering that it weakens the system of concepts, principles and foundations of data protection; unduly and excessively expanding the regulated scope; including insufficiently parameterized national defense, state security and intelligence activities; suppressing the entire framework of transparency and control over the processing of personal data in the criminal sphere; suppressing the entire framework for monitoring technologies; excessively expanding the legal bases for data processing for the purposes under protection, the hypotheses of sharing between authorities and access to data held by private agents, with incentives for the precariousness of technological infrastructures; and weakening rights and protections regarding automated decisions (Azevedo *et al*. , 2022).

This bill disregarded the Preliminary Draft of the Personal Data Protection Law for Public Security and Criminal Prosecution (Anteprojeto..., 2020), a text whose drafting had a multisectoral and democratic participation, whose work started from the Act of the President of the Chamber of Deputies, of November 26, 2019 and which was presented to the Chamber of Deputies in November 2020. This Draft, which also has its raison d'être in the recognition of the legal gap arising from the LGPD (Brasil, 2018), considers that the need for legal certainty so that the bodies responsible for public security activities and criminal investigation/repression can exercise their functions more efficiently and effectively, must be reconciled with the procedural guarantees and fundamental rights of the data subjects involved. Thus, it seeks to balance the protection of the data subject against misuse and abuse and the access of authorities to the full potential of modern tools and platforms for public security and investigations, considering that the lack of general regulation on the lawfulness, transparency or security of data processing in criminal matters, and of established rights or requirements for the use of new technologies that enable a degree of surveillance and monitoring unthinkable a few years ago, generates a very large asymmetry of power between State and citizen, which leaves the data subject without minimum normative guarantees and applicable institutional mechanisms to safeguard their personality rights, their individual freedoms and even the observance of due process of law.

3 METHODOLOGY

This section systematically covers the procedures used to carry out the research, describing in an organized way the techniques and strategies applied in its realization (Marconi; Lakatos, 2003). Thus, in relation to the question that seeks to answer the proposed study is characterized as exploratory, assuming a quali-quanti approach (Gil, 2002).

Gil (2002) explains that the exploratory study has an essential role in delimiting the research, as well as in formulating the problem. Cooper and Schindler (2011) point out that this procedure allows the researcher to conduct a preliminary survey of its object of study establishing familiarity with the theme, helping to determine what will be its focus.

The quantitative approach is due to the numerical data from the collection process involving the number of documents extracted from the databases. The qualitative approach is associated with obtaining an understanding of the documents found during the search process, establishing connections with the established research problem (Gil, 2002).

Thus, to investigate the works that address topics related to information monitoring and surveillance, as expressed in the theoretical framework, a literature review was carried out, seeking to identify which studies published between 2010 and 2020 have an intersection with information monitoring in the virtual environment. This literature review covered three databases: the Brazilian Digital Library of Theses and Dissertations (BDTD), Scopus and Web of Science.

Understanding the relevance of research reproducibility, it should be noted that the first procedure to be highlighted was the search process in the databases already explained, starting on November 30, ending on December 10, 2021. Chart 1 below summarizes the strategy adopted, making it possible to initially identify 39 articles, which resulted, after reading the title, keyword and abstract, in 19 documents relevant to the investigation. These articles are listed in Appendix A.

Chart 1. Database search strategy

Research objective	Verb	Identify		
	Action	Which studies published between 2010 and 2020 have an intersection with information monitoring in the virtual environment.		
Key words used	"Data" AND "Monitoring of Information" AND "Privacy" "Data" AND "Monitoring of Information" AND "Privacy"			
Search platforms	▪ Brazilian Digital Library of Theses and Dissertations (BDTD) ▪ *Scopus* ▪ *Web of Science*			
Methods applied for inclusion	BDTD Theses and dissertations published in English or Portuguese.	Scopus Articles published in English or Portuguese.	Web of Science Articles published in English or Portuguese.	
Methods applied for exclusion	BDTD Theses and dissertations published in a language other than that specified in the inclusion method, repeated documents, documents outside the scope determined by the search strategy.	Scopus Trials, expanded abstracts and articles published in a language other than that specified in the inclusion method, duplicate articles or outside the scope determined by the search strategy.	Web of Science Trials, expanded abstracts and articles published in a language other than that specified in the inclusion method, duplicate articles or outside the scope determined by the search strategy.	
Temporal cut-off	Period between 2010 and 2020			
Data analysis	Reading the title and abstract of the articles found for coding			
Preliminary results	39 documents			
Final result	19 documents			

Source: Survey data, 2021

Chart 1 summarizes the search strategy used in the literature review and explains the following questions:

a) Regarding the research objective, it is worth mentioning the relevance of understanding the advances in studies involving the theme proposed by Ball and Webster (2003), involving the monitoring of information flow in a virtual environment, thus the objective of the study seeks to identify which studies published between 2010 and 2020 have an intersection with the elements present in the monitoring of information in the virtual environment;

b) Regarding the choice of platforms, the Brazilian Digital Library of Theses and Dissertations (BDTD) records research at the master's and doctoral level, in which there is an immersion in the problem, given the objective and the time dedicated

to these works. The Scopus and Web of Science platforms were chosen due to their scope;

c) As for the inclusion methods in the BDTD database, it was decided to include dissertations and theses with language in English or Portuguese, related to the search strategies. In the Scopus and Web of Science databases, it was also decided to use only articles written in English or Portuguese, related to the search strategies;

d) The exclusion methods followed similar principles to those of inclusion, so in BDTD, dissertations and theses in a language other than Portuguese and English were excluded, as well as duplicate documents or outside the scope of the research. On the Scopus and Web of Science platforms, the same line of reasoning was followed, excluding duplicate articles, in a language other than Portuguese or English, as well as book chapters and expanded abstracts;

e) The temporal cut is justified by the period in which the studies proposed by Ball and Webster (2003) were carried out, aiming to identify the advances and intersections of the studies involving the theme;

f) The analysis process included reading the titles and abstracts, enabling the inclusion and exclusion procedure to be carried out, finally the complete reading of the documents for their coding;

g) The preliminary result contemplated 39 researches, being 18 documents from BDTD (6 theses and 12 dissertations), 15 articles from Scopus and 6 articles from Web of Science;

h) As a result of the process of reading the documents found, 4 theses and 2 dissertations were excluded from BDTD. The Scopus platform resulted in 9 exclusions of articles. The exclusion of the cited documents is associated with the reading carried out in full in which the researchers observed the lack of intersection between the strategies established for the searches in the databases. Finally, in the Web of Science, there were 5 exclusions. The result contemplated 19 researches related to the theme, being divided into 12 documents on the BDTD platform (2 theses and 10 dissertations), 6 articles on the Scopus platform and 1 article on the Web of Science platform.

The selected articles were then analyzed by the content analysis technique (Bardin, 2010), with the support of ATLAS.TI® software. Bardin (2010) explains that this technique consists of three phases covering:

1. The pre-analysis was evidenced in the procedure of searches, readings and screening of articles, dissertations and theses, found in the databases;
2. Coding was performed in the ATLAS.TI® software, after importing the selected documents after screening. The words data, information, monitoring, privacy and technology were used as codes, due to their adherence to the basic text of Ball and Webster (2003);
3. Finally, the treatment of the results, because after coding, a mechanical analysis of the selected texts began.

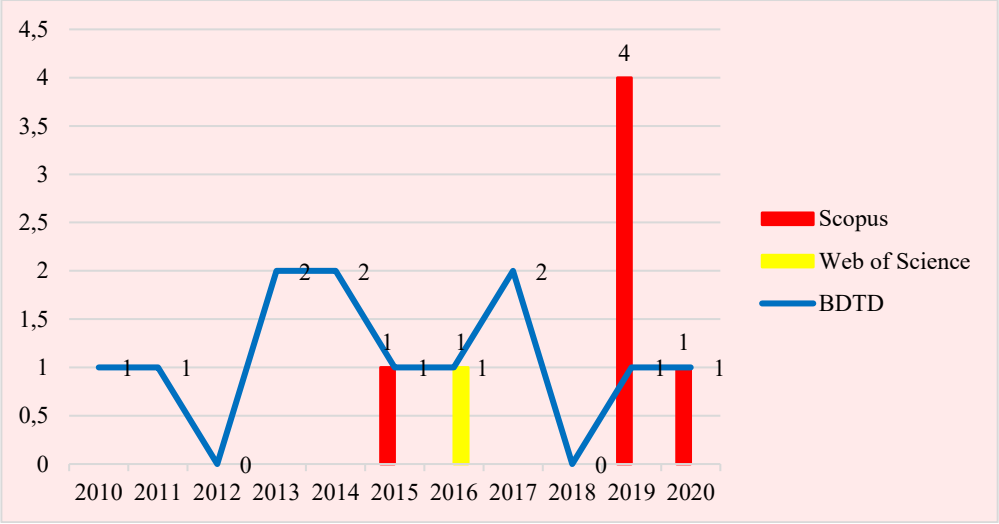
The phases listed by Bardin (2010) were significant, providing a strategy to answer the proposed research problem. Closing the collection process, the documents present in Appendix A were exported to the ATLAS.TI® content analysis software, where coding was used, involving the following words: - Data; - Information; - Monitoring; - Privacy; - Technology.

Regarding the words applied as codes in the content analysis performed in ATLAS.TI®, it is possible to observe their adherence with the related elements, among them is the basic text proposed by Ball and Webster (2003), a factor resulting from different analyzes, directing the research to analyze results and later to conclude the work.

4 ANALYSIS AND DISCUSSION OF RESULTS

The nineteen selected papers are unevenly distributed across platforms and also over the period analyzed. There are 12 works among theses and dissertations, 6 articles published in the Scopus database and only 1 article in the Web of Science database. The time distribution of the selected papers is shown in Graph 1.

Graph 1. Period of publications X quantity published



Source: Survey data, 2021

Between 2010 and 2013, no articles were identified that adhered to the objects of the research; the 4 works found are all on the BDTD platform, published in 2010 (1 article), 2011 (1 article), 2013 (2 articles). In 2014, 1 article was published in Scopus and 2 papers were registered on the BDTD platform. Between 2015 and 2018 no article was identified in Scopus and only 1 in Web of Science in 2016. In fact, no work was identified in 2018, as had already happened in 2012. In 2019, changing the scenario, 4 articles were published in Scopus, accompanied by 1 work in BDTD. In 2020 there are 2 papers, 1 in the Scopus base and 1 in the BDTD platform. (2 articles). There were no publications in 2012.

These data indicate that this theme has been the subject of research at master's and doctoral level, but the work carried out has not yet been published in journals. The distribution over time, and even the type of work found (12 theses and dissertations in BDTD, only 7 articles in Scopus and Web Of Science), with a greater concentration towards the end of the period consulted, seem to indicate that the theme is only now attracting greater attention from the community (in the terms established by the methodology). There seems to be a latent need for further investigation of the issue of monitoring/surveillance, in its different expressions, with regard to privacy and individual rights, also considering the different needs and expectations of society, expressed or not in legal statutes.

Separating the data according to the platform of origin, the analysis explained in Table 1 below covers the base of the Digital Library of Theses and Dissertations, where the codifications related to the content analysis of each document are analyzed.

Table 1. Frequency of recurrence of the codifications in the documents of the BDTD database.

Codes	Total frequency	Relative Frequency
Technology	44985	9,63%
Monitoring	58546	12,54%
Privacy	80983	17,34%
Information	107731	23,07%
Data	174769	37,42%

Source: Survey data, 2021

Observing the recurrence of the codes present in Table 1, it is relevant to highlight 3 points involving the data to information and the privacy of this informational flow, due to the number of times in which these terms appear in the analyzed documents, confirming the concern reported by Hoffmann (2011) in relation to the monitoring of the informational flow. Regarding the relative frequency column, it sought to highlight the percentage of each coding, making it easier to perceive the relevance of each coding in the context of the researched theme.

Following this line of reasoning, the Scopus base, the data in Table 2, covers another analysis resulting from ATLAS.TI®, making it possible to verify the frequency of recurrence of the codifications.

Table 2. Frequency of recurrence of codifications in Scopus documents.

Codes	Absolute Frequency	Relative Frequency
Privacy	1304	8,91%
Monitoring	2002	13,68%
Data	2448	16,73%
Technology	3990	27,26%
Information	4892	33,42%

Source: Survey data, 2021

The search processes in the Scopus database resulted in 6 articles, in which the frequency of recurrence of the codifications used was analyzed. Thus, it was possible to verify that the information appears with a higher degree of intensity in relation to the other themes worked on. As for the publication period of each document, it is important to emphasize that there was 1 publication in 2015, 4 publications in 2019 and 1 in 2020, related to the research proposal. This procedure made it possible to understand the concept explained by Choo (2003), about the role of information in human and organizational relations.

Finally, the analysis process ends by presenting the quantitative variables of the data obtained on the Web of Science platform and analyzed in ATLAS.TI®, as can be seen in Table 3 below.

Table 3. Frequency of recurrence of the codifications in the documents of the Web of Science database.

Codes	Absolute Frequency	Relative Frequency
Monitoring	103	10,25%
Technology	174	17,31%
Data	213	21,19%
Privacy	223	22,19%
Information	292	29,05%

Source: Survey data, 2021

Table 3 presents the data extracted from the Web of Science database, where information was evidenced as the most relevant element among the other codifications, however it is important to highlight that when addressing the use of applications to collect data

on a person's state, privacy assumes a significant role in this context. Thus, it is relevant to highlight that the Web of Science platform presented only one article, where the themes are related to the search strategies described in Table 1.

Thus, it showed higher levels of adherence to issues related to information and its privacy, with a higher concentration of recurrence among the codifications. Information is a relevant element among the other codifications, and it should be noted that when addressing the use of applications to collect data on a person's condition, the issue of privacy assumes a significant role in this context. This point allows us to return to the issue of global interconnection in the virtual environment, highlighted by Lévy (2008) the speed of propagation of this flow informed by Cella and Rosa (2013), factors that culminate in the key point of the theme addressed by Ball and Webster (2003) covering the monitoring and privacy of information in this environment.

5 CONCLUSION

After analyzing the data collected in each database and worked on the content analysis software ATLAS.TI® and Excel®, it is important to return to the objective established for this article - to identify which studies published between 2010 and 2020 have an intersection with information monitoring in the virtual environment. The research resulted in 19 documents, related to the purpose established by the researchers, making it possible to list the quantitative variables.

However, it is worth mentioning the qualitative perceptions, captured during the coding process, responsible for guiding the authors' conclusions in relation to the analyzed documents. It was possible to perceive among the research analyzed a need to monitor the information circulating in the virtual environment, involving the sender and receiver, due to different factors, covering security issues, increased data volume, new technologies, cybercrime, among other issues. However, monitoring extends beyond these purposes due to the volume of information circulating in this environment, seeking to avoid illegalities, as well as the dissemination of private data, as can be seen by analyzing the table in Appendix A, which highlights the relationship between the platforms, themes, year and titles of the articles adhering to the research. The number and distribution of articles over the period analyzed indicate that these topics require further research, especially considering the warnings of Ball and Webster (2003) and Henschke (2017) and the gaps in the legal regulations.

Finally, this work presents relevant contributions when analyzed from a social context, as it lists the relevance of information monitoring and its applicability to data privacy. Thus, it is possible to verify its contribution to Information Science by highlighting the issues that cover the flow of data in the virtual environment, as they result in different information for virtual users, with reflections on activities that take place in the physical environment, in the operations of organizations and in people's lives.

REFERENCES

ANTEPROJETO de Lei de Proteção de Dados para segurança pública e persecução penal. Brasília, 2020. Available at: http://bit.ly/3rxXfwe. Access on:23 jul. 2023.

ASSMANN, H. A metamorfose do aprender na sociedade da informação. **Ciência da informação**, Brasília, v. 29, p. 07-15, 2000. Available at: https://www.scielo.br/j/ci/a/ShzKdLbqJDPfssvSw9xWPrw. Access on:14 dez. 2021.

AZEVEDO, C. P. G. de *et al*. **Nota técnica**: análise comparativa entre o anteprojeto de LGPD penal e o PL 1515/2022. Instituto de Referência em Internet e Sociedade (IRIS) e Laboratório de Políticas Públicas e Internet (LAPIN), novembro de 2022. Available at: https://tinyurl.com/brmkxym6. Access on:20 jul. 2023.

BARDIN, L. **Análise de conteúdo**. São Paulo: Edições 70, 2010.

BALL, C; WEBSTER, F. **The intensification of surveillance**: crime, terrorism and warfare in the Information age. London: Pluto Press, 2003.

BARRETO, Aldo de Albuquerque. A questão da informação. **São Paulo em perspectiva**, São Paulo, v. 8, n. 4, p. 3-8, 1994. Available at: https://binged.it/3OvEZeg. Access on:08 nov. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, 2018. Available at: https://tinyurl.com/ye2ydbm9. Access on:08 nov. 2021.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Brasília, 2019. Available at: https://tinyurl.com/4ejwzcf4. Access on:08 nov. 2021.

BRASIL. Câmara dos Deputados. **PL 1515/2022**: Projeto de Lei de Proteção de Dados Pessoais para fins exclusivos de segurança do Estado, de defesa nacional, de segurança pública, e de investigação e repressão de infrações penais. Brasília, 2022. Available at: https://www.camara.leg.br/propostas-legislativas/2326300. Access on:22 jul. 2023.

CALDEIRA, C; SARLET; G. B. S. O consentimento informado e a proteção de dados pessoais de saúde na internet. **Civilistica.com**, Rio de Janeiro, v. 8, n. 1, p. 2-27, 2019. Available at: https://run.unl.pt/handle/10362/94969. Access on:17 nov. 2021.

CANONGIA, C; MANDARINO JUNIOR, R. Segurança cibernética: o desafio da nova Sociedade da Informação. **Parcerias Estratégicas**, Brasília, v. 14, n. 29, p. 21-46, 2010. Available at: https://tinyurl.com/ybnbn52j. Access on:15 dez. 2021.

CAPURRO, R; HJORLAND, B. O conceito de informação. **Perspectivas em ciência da informação**, Belo Horizonte, v. 12, p. 148-207, 2007. Available at: https://www.scielo.br/j/pci/a/j7936SHkZJkpHGH5ZNYQXnC. Access on:11 nov. 2021.

CARANDINA, T. Da gestão da informação ao comportamento informacional. **Revista Científica Multidisciplinar**, São Paulo, v. 2, n. 3, p. 20-35, 2021. Available at: https://recima21.com.br/index.php/recima21/article/view/133. Access on:22 abr. 2022.

CORTELLA, M. S. **Qual é a tua obra**? Inquietações propositivas sobre gestão, liderança e ética. Rio de Janeiro: Vozes, 2017.

CELLA, J R. G; ROSA, L. A. S. Controle social e necessidade de proteção de dados pessoais. **Revista de Direito Brasileira**, Passo Fundo, v. 6, n. 3, p. 216-231, 2013. Available at: https://indexlaw.org/index.php/rdb/article/view/2748. Access on:11 nov. 2021.

CHOO, C. W. A **Organização do conhecimento**. São Paulo: Editora Senac São Paulo, 2003.

COOPER, D. R.; SCHINDLER, P. S. **Métodos de pesquisa em administração.** 7. ed. Porto Alegre: Bookman, 2003.

DAMIÃO, A. K. **Guerra cibernética**: proteção cibernética monitoramento de redes e sistemas e levantamentos de vulnerabilidades. 2018. Trabalho de Conclusão de Curso (Especialização em Ciências Militares com ênfase em Gestão Operacional). Escola de Aperfeiçoamento de Oficiais, Rio de Janeiro, 2018. Available at: https://tinyurl.com/y27jr4sx. Access on:18 nov. 2021.

FREITAS, H. *et. al*. **Informação para a decisão.** Porto Alegre: Ortiz, 1997.

GIL, A. C. **Como elaborar projetos de pesquisa.** 4. ed. São Paulo, Atlas, 2002.

GOULART, L. **A criação de perfis falsos por agentes policiais para investigação do crime de tráfico de drogas no ambiente virtual com base na Lei nº 13.964/2019**. 2021. Trabalho de Conclusão de Curso (Bacharel em Direito). Universidade do Sul de Santa Catarina, Tubarão, 2021. Available at: https://tinyurl.com/vhbwuktf. Access on:19 dez. 2021.

HENSCHKE, A. **Ethics in na age of surveillance**: personal information and virtual identities. Cambrige: Cambridge University Press, 2017. ISBN 978-1-107-13001-2.

HOFFMANN, W. A. M. Monitoramento da informação e inteligência competitiva: realidade organizacional. **InCID**: Revista de Ciência da Informação e Documentação, São Paulo, v. 2, n. 2, p. 125-144, 2011. Available at: https://www.revistas.usp.br/incid/article/view/42356. Access on:17 de out. 2021.

LÉVY, P. **Cibercultura.** São Paulo: Editora 34, 2008.

LIMA, J. D. **Discurso de ódio em ambiente virtual: contribuições da gestão da informação para aumento da eficiência na investigação policial.** 2020. Dissertação (Programa de Mestrado em Ciência da Informação). Universidade Federal de Santa Catarina, Santa Catarina, 2020. Available at: https://tinyurl.com/bd8fbnsw. Access on:19 nov. 2021.

MALVEIRA, A. C. A Espetacularização da identidade virtual nas redes sociais. *In*: CONGRESSO DE COMUNICAÇÃO DA REGIÃO SUL, 12., 2011, Londrina-PR. **Anais do** [...]. São Paulo: Intercom, 2011, p.1-13. Available at: https://tinyurl.com/yvmh6kcf. Access on:05 dez. 2021.

MARCONI, M. A.; LAKATOS, E. M. **Fundamentos de metodologia científica.** 5. ed. Ed. Atlas. São Paulo, 2003.

MELO CUNHA, B. E. *et al*. As dificuldades da implementação da LGPD no Brasil. **Revista Projetos Extensionistas**, Pará de Minas, v. 1, n. 2, p. Available at: https://periodicos.fapam.edu.br/index.php/RPE/article/view/391. Access on:19 dez. 2021.

MONTEIRO, R. L. Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil. **Artigo estratégico,** Rio de Janeiro, v. 39, p. 1-14, 2018. Available at: https://bit.ly/2K0TcS5. Access on:19 dez. 2021.

RAZZOLINI FILHO, E. **Introdução à gestão da informação:** a informação para organizações no século XXI. Curitiba: Juruá, 2020.

SANTOS, D. F.; SANTOS, M. C.; SANTOS, A. F.; MOREIRA, A. L. D. Análise do processo da tomada de decisão em empresas familiares. **Administração de Empresas em Revista**, São Paulo, v. 4, n. 26, p. 162-181, 2021. Available at: http://revista.unicuritiba.edu.br/index.php/admrevista/article/view/4925. Access on:20 abr. 2022.

VAN DIJCK, J. Confiamos nos dados? As implicações da datificação para o monitoramento social. **Matrizes**, São Paulo, v. 11, n. 1, p. 39-59, 2017. Available at: https://www.redalyc.org/pdf/1430/143050607004.pdf. Access on:10 dez. 2021.

Appendix A

Chart 2. List of platforms and articles included in the research

Platform	Theme	Year	Title	Author (s)
BDTD (Dissertation)	Sending and receiving data and its impact on users' privacy.	2020	A defense mechanism against temporal side-channel traffic attacks in the context of IoT.	Prates Junior.
BDTD (Dissertation)	Implementation of the electronic medical record in the Single Health System.	2019	Implementation of the electronic medical record in primary care in the Unified Health System: results of PEMAQ AB 2011 and 2014.	Velloso.
BDTD (Thesis)	It analyzes the complex environment of social networks and their interactions, where information exchange takes place.	2017	Data collection in social networks: Privacy of personal data in access via Application Programming Interface	Rodrigues.
BDTD (Dissertation)	It addresses the main search engines developed over time.	2017	The communicative evolution of search engines: from telegraph to semantic web.	Toth.
BDTD (Dissertation)	Monitoring information in the cloud and its relation to storage and privacy issues.	2016	Trust-based architecture for file integrity verification in computational clouds.	Pinheiro.
BDTD (Thesis)	The application of new technologies to improve the security of files stored in the cloud.	2015	Cloud computing management using security criteria.	Silva.
BDTD (Dissertation)	The implementation of noise in the quest to preserve privacy without losing the usefulness of the data.	2014	Preserving privacy in Smart Grids through noise addition.	Barbosa.
BDTD (Dissertation)	Mechanisms used to ensure the privacy of the user who has data stored in the cloud, when it is accessed.	2014	Cloud-based mechanism for monitoring sensitive data.	Souza.
BDTD (Dissertation)	Improved information security during the process of collecting data stored in the cloud.	2013	An architecture for security monitoring based on service level agreements for infrastructure clouds.	Ferreira.
BDTD (Dissertation)	Study of cyberspace involving territorial issues and the monitoring of information of users operating in this environment.	2013	Cyberspace as a geographical category.	Silva.
BDTD (Dissertation)	It studies the rise of social networks and the interactions that occur in this environment between users and e-commerce, highlighting the issue of consumer rights and issues such as data privacy.	2011	Cyberspace law and social networks: challenges of consumer protection in social commerce.	Barreto.
BDTD (Dissertation)	It involves the expansion of data flow, related to information on health professionals.	2010	Proposal for online management of epidemiological surveillance information on adverse events following immunization.	Silva Junior.

Scopus	This research seeks to explore and demonstrate the application of blockchain and smart contract technologies to innovate/renew home care services to reap the desired benefits of blockchain of transparency of the data collection process by making the procedure automated.	2020	Development and evaluation of a smart contract–enabled blockchain system for home care service innovation: mixed methods study.	Chang; Chen; Lu; Luo.
Scopus	The research consists of the use of open data, focused on tourism, involving the connection of different interfaces, meeting the need for information about citizens and tourism.	2019	A Cloud information monitoring and recommendation multi-Agent system with friendly interfaces for tourism.	Chen; Yang.
Scopus	It studies the monitoring of an online emergency system, in which it seeks to identify whether there is an invasion of user privacy.	2019	Acceptance of Smart electronic monitoring at work as a result of a privacy calculus decision.	Princi; Kramer.
Scopus	The research involves a model for security risk assessment in the supply chain, since in this environment there is interaction with different interfaces, generating a large volume of information.	2019	CSCCRA: A novel quantitative risk assessment model for SaaS cloud service providers.	Akinrolabu; New; Martin.
Scopus	The research involves issues that cover the violation of personal information in the collection procedures.	2019	Privacy-aware blockchain for personal data sharing and tracking.	Onik; Kim; Lee; Yang.
Scopus	It addresses the study of social media and information sharing among professionals.	2015	A method of designing a generic actor model for a professional social network.	Ninawe; Venkataram.
Web of Science	Study on the collection of information by pregnancy apps.	2016	An Australian survey of women's use of pregnancy and parenting apps.	Lupon; Pederson.

Source: Survey data, 2021