

Scientific Journal of Applied Social and Clinical Science

RESEARCH BODIES AND THE ADOPTION OF PRIVACY SINCE CONCEPTION

Márcia Soares da Cunha

``Universidade de Brasília``, Post-graduation
Program in Intellectual Property and
Technology Transfer for Innovation
PROFNIT, Brasília – DF, Brazil
<http://lattes.cnpq.br/0343056953174178>
<https://orcid.org/0000-0003-4653-4801>

Patrícia Regina Sobral Braga

``Universidade de Brasília``, ``Faculdade
UnB Gama`` (FGA), Energy Engineering,
Post-graduation Program in Intellectual
Property and Technology Transfer for
Innovation
PROFNIT, Brasília – DF, Brazil
<http://lattes.cnpq.br/9929982133650606>
<https://orcid.org/0000-0003-0149-3663>

All content in this magazine is
licensed under a Creative Com-
mons Attribution License. Attri-
bution-Non-Commercial-Non-
Derivatives 4.0 International (CC
BY-NC-ND 4.0).



Abstract: This article aimed to carry out a prospective study on the topic of privacy, aiming to identify the relevance of the subject and the main related technological areas. Using a methodology involving four steps, academic production and patent registration involving the topic were identified. There was considerable academic production on the topic, especially in 2022, and an increase in patent filings, mainly in subclasses H04 and G06 of the international patent classification. The positive and negative aspects of adopting privacy principles were systematized through a SWOT matrix, considering the importance of the topic for research bodies, both as a field to be explored in various technological areas, and for the application of research involving data personal. It was concluded that the topic is relevant, not only due to the need for compliance, but also to mitigate risks arising from inadequate treatment.

Keywords: Privacy. Research bodies. Patents.

INTRODUCTION

Technological advances are associated with disruptive processes and procedures that have changed the global production system. In this context, the first three industrial revolutions were triggered by innovations such as the introduction of mechanical manufacturing powered by water and steam, at the end of the 18th century; the division of labor in a production line, idealized by Henry Ford, at the beginning of the 20th century and the introduction of logically programmable controllers, for the purpose of manufacturing automation, in the early 1970s (BRETTEL et al., 2014).

Such advances were even faster following the fourth industrial revolution, which established a new era of economic and social transformations, with the spread of the internet, including mobile, high connectivity between devices and modern sensors. Thus,

innovations in the scope of Information and Communications Technology (ICT) motivated the establishment of a digital economy, in which human beings and intelligent objects interact and are capable of making decisions, providing faster and more accurate production methods. The internet of things, decision support systems, big data, cloud storage and artificial intelligence, among others, emerge as drivers of digital transformations in business models, providing the basis for optimized and resilient execution (ZIMMERMANN et al., 2016).

In a globalized and interconnected market, large volumes of data circulate across national borders in a continuous flow of long and complex value chains. The free movement of information in the form of data is called “free flow of data” and its importance is recognized by leading countries in the digital economy and international organizations. The Organization for Economic Cooperation and Development (OECD) even considers that this data-driven technological ecosystem will be one of the engines of economic growth in the 21st Century. The Organization has been dedicated to debating the topic since the beginning of 1980, when it prepared the recommendations for the Guidelines on the protection of Privacy and Transborder Flows of Personal Data, a document later updated in 2013 (BRAZIL, 2018a, p. 38).

As the digital universe is based on data, sometimes handled in large volumes with the aim of generating information, it is imperative to adopt measures to protect it, in order to avoid risks for organizations and, if it is personal data, to protect the rights of their holders. Therefore, the greater the volume of data transmitted, the greater the risk that may arise from an information security incident, and it is up to those who process it to adopt measures to prevent the exposure or use of data under their responsibility.

Thus, in this digital era, data has gained

great relevance and has become an asset for many organizations, which have it as the core of their business, as is the case with the company Google. Given this, as technology evolved, data capable of individually identifying a person became increasingly exposed, thus increasing the risk of invading the privacy of its holder (FERREIRA; PINHEIRO; MARQUES, 2021, p 156).

[...] Risk that materializes in the possibility of exposure and improper or abusive use of personal data, in the event that these data are not correct and misrepresent their holder, in their use by third parties without their knowledge, just to mention some real hypotheses. It is therefore necessary to establish mechanisms that enable people to have knowledge and control over their own data – which, in essence, are a direct expression of their own personality. For this reason, the protection of personal data is considered in several legal systems as an essential instrument for the protection of the human person and as a fundamental right (DONEDA, 2011, p. 92).

It is worth noting that concerns about privacy are not a topic that emerged in the digital era, according to Ferreira et. al. (2021), the idea of full protection of the individual, both from a personal and property point of view, goes back to 1890, with the publication of the article entitled “The right to privacy” by jurists Samuel D. Warren and Louis D. Brandeis, “in which the authors argue that civil rights must encompass the protection of private life, not only property, but also the protection of the well-being and peace of mind of individuals” (FERREIRA; PINHEIRO; MARQUES, 2021, p. 157). Thus, from the advancement of the digital era to the protection of personal data, a trajectory was established that culminated in the current maturity of the topic, addressed in global legislation, worth highlighting: the American Declaration of the Rights and Duties of Man, held in Bogotá, in 1948, during the IX American International

Conference; the International Covenant on Civil and Political Rights, approved in 1966, but which only came into force in 1976; and the American Convention on Human Rights, known as the Covenant of San José, Costa Rica, in 1969, among others (FERREIRA; PINHEIRO; MARQUES, 2021, p. 159).

Doneda (2011) highlights that, according to the classification proposed by Viktor Mayer-Schönberger, four generations of laws demonstrated the evolution of the focus given to the protection of personal data over time. We can highlight the General Data Protection Regulation (GDPR) of the European Union (EUROPEAN UNION, 2016), which sought to overcome the disadvantages of individual approaches existing in legislation until then, establishing a collective standard for the protection of personal data (DONEDA, 2011, p. 98).

This regulation came into force in 2018 and put Europe in the spotlight, where the GDPR addresses the rights to transparency, information, access, rectification, deletion, forgetfulness and the right to object, limitation of processing and data portability (FERREIRA; PINHEIRO; MARQUES, 2021, p. 163).

Inspired by European legislation, Brazil, joining other countries, regulated the fundamental right to protection of personal data, through a general law that regulates the subject (BRAZIL, 2018b), as well as registering such protection in the Constitution of the Federative Republic of Brazil (BRAZIL, 1988). In this sense, in 2020, the General Personal Data Protection Law (LGPD) (BRAZIL, 2018b) came into force, including the holder of personal data at the center of relationships involving their data, in order to protect them from abuse and promote risk mitigation to citizens’ fundamental rights, especially human dignity, privacy and freedom.

Privacy and intimacy, in these terms, are integral parts of personality rights,

protecting the possibility of every person to exclude from the knowledge of third parties that which only refers to them and which concerns the scope of their private life, aiming at moral integrity of the human being. Thus, these rights imply a duty to all other people not to disclose the privacy of others and not to interfere in it, including the Public Administration (PIRONTI; ZILLOTTO, 2021, p. 414).

Thus, the protection of personal data in Brazil has become an essential tool to guarantee the right to privacy, that is, the right to “be left alone”, to have the inviolability of one’s private life assured and to be able to exercise informational self-determination over one’s privacy. personal data.

[...] autonomy of the individual in the informational society and suggests a new concept of privacy, that is, from the historical definition of the “right to be left alone” to the “right to informational self-determination”. This concept encompasses the right to maintain the control over your own information; the right to choose what will be revealed; right to be forgotten, in short, the right to determine the way to construct one’s own private sphere (BARROS; BARROS; OLIVEIRA, 2017, p. 19).

In this context, the LGPD, in addition to ensuring rights for holders of personal data, establishes obligations for those responsible for processing personal data, which the LGPD calls “processing agents”.

Such agents must adopt technical and administrative measures to protect the personal data under their supervision, in order to guarantee the privacy of their holders. The LGPD establishes legal hypotheses that authorize the processing of personal data to be carried out by processing agents, such as processing to carry out studies by research bodies, guaranteeing anonymization whenever possible (BRAZIL, 2018b).

Consistent with the Innovation Law (BRAZIL, 2004), the LGPD incorporated the

concept of research bodies and the National Data Protection Authority (ANPD), a special agency responsible for ensuring the application of the LGPD, and carried out studies on the performance of the bodies research in compliance with LGPD.

[...] direct or indirect public administration body or entity or non-profit private legal entity legally constituted under Brazilian laws, with headquarters and jurisdiction in the country, which includes basic or applied research in its institutional mission or social or statutory objective of a scientific or technological nature or the development of new products, services or processes (BRAZIL, 2004) (this section was highlighted by us).

In such a study, the ANPD emphasizes that the legal basis for carrying out studies by research bodies is applicable by the research body, not by individual researchers.

[...] the agent legitimized to use the legal basis under study is the research body itself, be it a public body or entity or a non-profit legal entity governed by private law. Therefore, the use of this legal basis by natural persons acting in their own name or without any connection with a research body is not permitted (ANPD, 2022, p. 17).

In the same sense, the responsibility for the processing of personal data lies with the research body, which must know the activities carried out by its researchers.

The art. 13 of the LGPD reinforces this interpretation, by expressly mentioning that “research bodies may have access to personal databases, which will be treated exclusively within the body”. In the same vein, § 2 of art. 13 establishes that “the research body will be responsible for information security [...]”. It is clear, therefore, that the responsibility for the processing of personal data carried out for the purposes of studies and research, including in the field of public health, is of an institutional nature, in the sense that it is legally attributed to the research body itself (ANPD, 2022, p. 18).

[...] according to the LGPD, the responsibility for the processing of personal data in the cases provided for in arts. 7th, IV and 11, II, c, will always belong to the research body – and not to the natural persons subordinate or linked to it, such as researchers, scholarship holders and undergraduate or postgraduate students. It is, in other words, a responsibility of an institutional nature, which is legally attributed to the research body itself (ANPD, 2022, p. 21).

For this reason, the research body must sign a term of commitment with the researchers, which establishes the limits of the processing of personal data and responsibilities.

Specifically, in the case of public entities and bodies that provide access to personal data for study and research purposes, it is understood that, without prejudice to compliance with other applicable legal requirements, such as the provisions of the LAI, proof of the researcher's relationship with the research body can be carried out by simply presenting a formal document, such as, for example, a “term of science and responsibility”. This document must attest to the knowledge of the research body regarding the carrying out of the study and compliance with the relevant obligations set out in the LGPD, in particular the linking of the use of data to the purpose of carrying out the study and the commitment to adopt prevention and security appropriate to the case (ANPD, 2022, p. 18).

Therefore, in the exercise of their activities, research bodies must adopt the legal basis for processing personal data to carry out studies by research bodies, considering themselves responsible for the research carried out by the people linked to them, observing the principles of the LGPD, the relevant ethical standards, according to the object of the research that involves the processing of personal data, as well as ensuring the security of the data processed.

More than the organization's compliance with the LGPD, research organizations when

carrying out studies involving personal data must observe the principles of privacy by design. These principles help ensure information security for the protection of personal data, consisting of guidelines to be incorporated into all processes, as shown in Figure 1.

These principles guide the adoption of good practices to provide privacy from the conception of a project and throughout the life cycle of the personal data included in it. Thus, organizations, especially research bodies, when incorporating such principles comply with the legislative command that establishes that, when processing personal data, bodies must adopt technical and administrative measures to protect personal data (BRAZIL, 2018b).

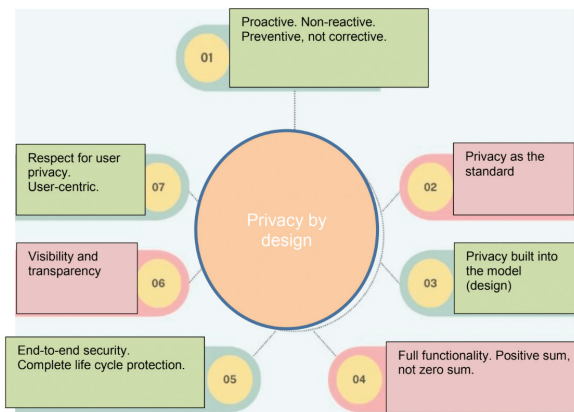


Figure 1: Privacy Principles by Design.

Source: The authors (adapted from BRAZIL, 2020), 2023.

In view of recent legislation and its possible implications on the processes of research bodies, the research problem is to identify how the topic of privacy has been impacting scientific and technological production, especially since 2018, when the legislation came into force of the European Union and Brazilian law was sanctioned.

To this end, the study's general objective is to carry out a prospective study on the topic of privacy, aiming to identify the relevance of the subject and the main technological areas

related to the topic. The effort used is justified as a way of understanding the evolution of the topic, especially due to its effects on scientific production and patent registration.

To meet this general objective, the following specific objectives were established: (1) identify the evolution of articles published on the topic of privacy; (2) identify the registration of patents on the subject of privacy; (3) qualitatively analyze the summaries of available patents involving the topic of privacy in Brazil; and (4) propose a diagnosis of challenges and opportunities involving the adoption of privacy from the conception of a project through a SWOT matrix.

METHODOLOGY

The adoption of a methodological process based on exploratory and descriptive research was fundamental to achieving the objectives of this work.

The data was obtained from categorized sources and the mappings were obtained from a bibliometric study that used data and text mining as a data processing mechanism.

The research employed a methodology consisting of four stages presented in Figure 2.

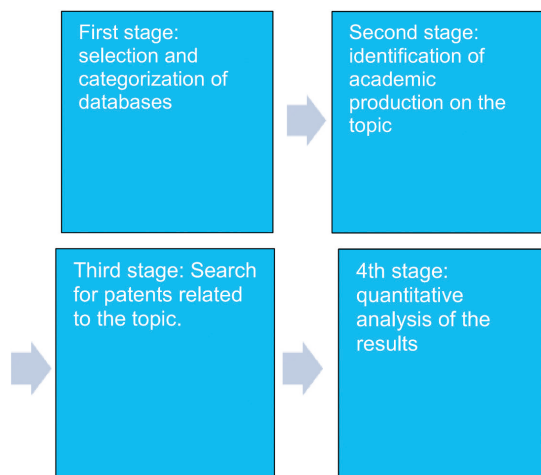


Figure 2: Research methodological structure.

Source: The authors, 2023.

In the first stage, the databases were

selected and categorized. To identify academic production, the journal portal of the Coordination for the Improvement of Higher Education Personnel (CAPES) was selected. The result generated was categorized by type of resource and date of creation. To search for patents, the databases of the World Intellectual Property Organization (WIPO Patent scope) and the National Institute of Industrial Property (INPI) were used. These two bases were chosen for their international and national projection, respectively.

In the second stage, academic production on the topic was identified from the CAPES journal portal. The search in the collection was carried out by subject, applying the type of resource “article” as a filter, whose title contained the word “privacy”. The Boolean OR operator was used for a more accurate result, since the search did not restrict language or period. Based on the results obtained, annual refinements were carried out in order to identify whether academic production was affected by the publication of the Brazilian law on the protection of personal data (BRAZIL, 2018b) which occurred in the same year as the entry into force of European legislation (EUROPEAN UNION, 2016) on the topic.

In order to also evaluate publications involving aspects of privacy by design, known internationally by the term “privacy by design”, the Boolean operator (AND) and the term “design” were incorporated into the result.

In the third stage, using the WIPO Patent scope and INPI bases, patents were identified, in which the search terms are presented in Table 1.

Data base	Search terms
WIPO Patent scope	Advanced search – term: “privacy” – in title – language: “English”
INPI	patents – “contain any of the words” – “privacy” OR “privacy” – “in the title”

Table 1: Patent search terms in the studied databases.

Source: The authors, 2023.

Given the number of results found in both databases, the highest occurrence of patents by code of the international patent classification (CIP) was identified, in order to establish a standard that would allow comparing the annual incidence of patent filings involving the topic of privacy.

In the fourth stage, the results found were analyzed in order to evaluate the information on the topic of privacy and carry out a diagnosis of opportunities and threats materialized in a SWOT matrix.

RESULTS AND DISCUSSION

The academic production involving the topic of privacy was obtained from research on the CAPES journal portal, resulting in 46,758 articles containing the word “privacy” or “privacy” in their title, of which 26,828 occurred between 2014 and 2022.

In order to identify whether legislation on the topic had an impact on the preparation of articles, annual filters were applied in order to segment the data from 2014 onwards. As can be seen in Figure 3, until 2016, the year of publication of European legislation, the values did not change significantly, but showed considerable growth in the following years.

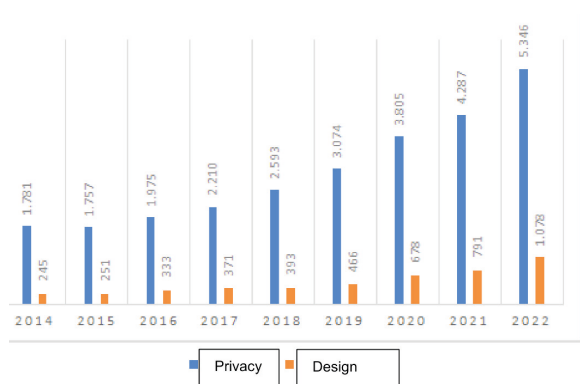


Figure 3: Total articles published on the topic of privacy from 2014 to 2022.

Source: The authors, 2023.

To verify adherence to the concept of privacy by design, the search was refined

using the Boolean operator AND, and the term “design”. This way, it can be seen that among the total number of articles published, 6,433 included the term “design”, of which 4,606 were published between 2014 and 2022, indicating that privacy as a whole and its implementation since conception is the subject of academic studies. Furthermore, it was possible to verify that 2,421 articles have already been published on the CAPES journal portal this year, indicating that the topic remains relevant.

Regarding the search for patents, Table 2 presents the results observed for the identification of patents in the WIPO Patent scope and INPI databases.

Data base	Search result for patents with title privacy or privacy
WIPO Patent scope	11,503
INPI	74

Table 2: Results observed in the patent search in the studied databases.

Source: The authors, 2023.

The search carried out on the WIPO Patent scope returned 11,503

results through the use of filters using the Boolean operator AND (period: 2014 to 2022 and English language and title containing the word privacy). Table 3 explains the results of this research.

Among the countries that had the largest number of patents filed, the United States, China and India stand out, as well as the European Patent Office.

Figure 4 shows the evolution of the number of patents filed in the three countries that had the most significant results. Figure 4 makes it possible to observe an increase in the number of patents filed mainly from 2018 onwards, with its peak in 2021.

Year	2014	2015	2016	2017	2018	2019	2020	2021	2022	Total
Deposit	642	627	678	904	1.118	1.411	1.698	2.334	2.091	11.503

Table 3: Search result in the WIPO Patent scope database.

Source: The authors (adapted from WIPO Patent scope), 2023.

International Request	Year	Title	IPC
PCT/US2020/063359	2020	Privacy – preserving code delivery activation. for pseudonym certificates	H04L
PCT/US2020/054537	2020	Privacy and Efficiency Balancer for Revocation of vehicle public key infrastructure	H04L
PCT/BR2022/050140	2022	Smart Media protocol method, a media ID for accountability and authentication, and provision for security and privacy when using screen devices, to make messaging data more private	G06F

Table 4: Patents filed WIPO Patent scope with Brazil as the inventor’s country of origin.

Source: The authors (adapted from WIPO Patent scope), 2023.

Powers	Weakness
<ul style="list-style-type: none"> • Legal compliance; • Guarantee of holders’ rights; • Reducing data leakage risks; • Adequacy of business processes; • Establishing standards for new projects; • Cultural change in respect for privacy; • Adoption of security measures. 	<ul style="list-style-type: none"> • Lack of organizational culture regarding the processing of personal data; • Collection and storage of personal data in excess or without due legal compliance; • Reuse of personal data without the support of an adequate legal hypothesis; • Inadequate infrastructure for processing personal data securely.
Opportunities	Threats
<ul style="list-style-type: none"> • Possibility to take advantage of the principles of privacy in new inventions; • Existence of academic and scientific production on the topic; • Market demand for LGPD-compliant inventions; • Possibility of partnership with research bodies and scientific and technological institutions for the development of innovations in line with the theme 	<ul style="list-style-type: none"> • Suffer administrative and judicial sanctions; • Compromise of research deadlines due to external determinations that prevent the use of personal data; • Preventing the collection of personal data essential for the development of the study or research; • Invasion of databases by adverse agents (“hackers”)

Table 5: SWOT matrix of LGPD implementation from the conception of a project.

Source: The authors, 2023.

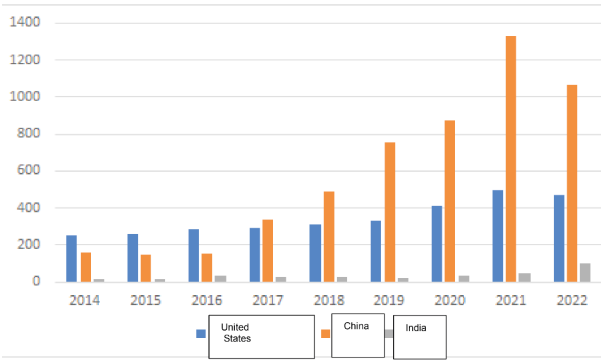


Figure 4: Result from the WIPO Patent scope database of the most significant countries.

Source: The authors (adapted from WIPO Patent scope), 2023.

Thus, in the WIPO Patent scope results, 6,067 occurrences were found with code G06F, which showed growth from 2016, the date of publication of European legislation, and its peak in 2021, as shown in Figure 5.

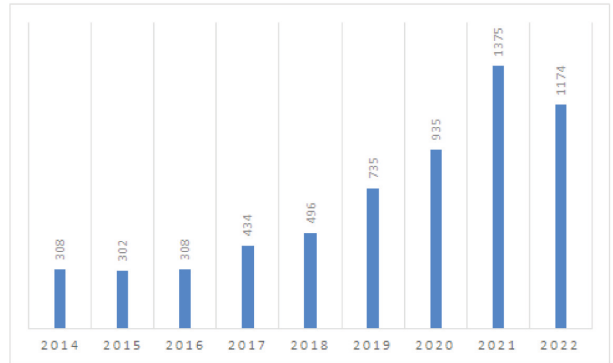


Figure 5: Annual search result in the WIPO Patent scope database refined by code G06F.

Source: The authors (adapted from WIPO Patent scope), 2023.

In the WIPO Patent scope database, Brazil is not listed as the country of origin of patent applications containing the word “privacy” or “privacy” in the patent title. However, when refining the initial result by adding the Boolean operator AND and the inventor’s country of origin as Brazil, three patents filed in the analyzed period were returned, through the Patent Cooperation Treaty (whose international acronym is PCT), which allows you to apply for patent protection simultaneously in several countries that are signatories to the treaty. Table 4 lists these patents, with the first two listing “Universidade de São Paulo” as the applicant.

Regarding the technology indicated in the filed patents, both the results of the search in the WIPO Patent scope database and in the INPI database, returned the highest concentration of deposits in subclasses H04 (Electricity – Electrical Communication Technique) and G06 (Physics – Calculation: Calculation or Counting)¹, mainly in code G06F – Electrical Processing of Digital Data, which is consistent with the fact that currently a large part of the data is processed in digital media.

Regarding the results of the search for patents in the INPI database, of the 74 patents found containing the term “privacy” in their title, 39 were from the period from 2014 to 2022, highlighting the year 2020 with 11 patents. Regarding the International Patent Code, the majority also focuses on the G06F code, totaling 16 patents filed.

It is important to highlight that, in the INPI database, five computer program records with the term privacy were also identified, including a privacy management system for small businesses (BR5120220008580) and one with the title “Privacy Unicamp” (BR5120220013495) both granted in 2022.

Despite the higher incidence in the G06F code, in the two databases analyzed, patent records were identified in different Patent Classification codes, which confirms that the topic of privacy is not restricted to the processing of data through digital means and that it is a transversal theme to other

1. http://ipc.inpi.gov.br/classifications/ipc/ipcpub/?notion=scheme&version=20230101&symbol=none&me_nulang=pt&lang=pt&viewmode=f&fipcp=no&showdeleted=yes&indexes=no&headings=yes¬es=yes&direction=o2n&initial=A&cwid=none&tree=no&searchmode=smart

technological areas, serving as an indication for researchers to pay attention to the topic of privacy in all their projects, as it can be a competitive differentiator if it involves the privacy of potential users of the technology.

Finally, based on the results found in data from academic production and patent searches, as well as considering the theoretical framework of this work, it was possible to measure the contributions of the topic to society, based on the elaboration of a SWOT matrix, which is a strategic research resource disseminated within management, through which it is possible to observe the internal and external environment of the business and structure guidelines to facilitate a global view of opportunities and threats that may exist, enabling greater competitiveness of the business or project (RIBEIRO, 2018).

When preparing the matrix, it was considered that the topic of privacy must be implemented from the conception of a project, especially by research bodies, when they use personal data in their projects, thus allowing analyzes to be carried out to identify weaknesses, opportunities, strengths and threats, related to the topic of privacy and legal compliance with the LGPD, as shown in Table 5.

As demonstrated in the matrix, the adoption of privacy principles from conception, in addition to legal compliance, makes the organization more competitive as it adheres to important legislation that aims to ensure the rights of holders of personal data.

For research bodies, it adds a difference by inserting personal data protection requirements from the beginning of the project, avoiding rework, controlling the actions of researchers who process personal data on their behalf, ensuring compliance with current legislation and respect the rights of personal data holders.

CONCLUSION

The present study aimed to carry out a prospective study on the topic of privacy, aiming to identify the relevance of the subject and the main technological areas related to the topic, which was carried out through exploratory and descriptive research based on academic production and registration of patents.

To obtain research data, a literature review was carried out in the CAPES journal database, which demonstrated an increase in the proposed theme in the period from 2014 to 2022. It is worth highlighting that in the period considered, the year 2022 had the largest number of articles published with the topic of privacy, totaling 5,346 articles, in different areas of knowledge. This number represents approximately triple the number of articles published in 2014 and approximately double the number of publications in 2018.

To search for patents, the WIPO Patent scope database in English and Portuguese and the INPI database were considered. From the results it can be observed that the technological areas with the highest incidence of patents filed involving the topic of privacy are subclasses H04 (Electricity – Electrical Communication Technique) and G06 (Physics – Computing: Calculation or Counting) of the international patent classification.

Furthermore, at WIPO Patent scope the filing of patents containing the subject of privacy in the English language was greater as of 2018 than in previous years.

Previous studies, with the Portuguese language the number of patents filed did not vary significantly.

Based on the INPI, the year 2020, in which Brazilian legislation came into force, recorded 11 patent filings among the 39 privacy-themed patents filed between 2014 and 2022.

Based on the data obtained, it was possible to identify that personal data protection

legislation affected both academic production and the filing of patents on the subject of privacy. In view of this, a SWOT matrix was created with a diagnosis of challenges and opportunities when implementing the LGPD from the conception of a project capable of providing a competitive advantage for projects involving the topic.

It is concluded, therefore, that the topic is relevant and current, both in a national and international context, demonstrating that

legislation affecting the topic has an impact on academic production and patent filings. Therefore, it is strategic to seek compliance with the LGPD and promote the adoption of privacy principles to provide a competitive advantage in technologies that involve the processing of personal data, promoting research that adheres to good privacy practices in order to guarantee the rights of its holders and legal compliance.

REFERENCES

- AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD). **Estudo Técnico - A LGPD e o tratamento de dados pessoais para fins acadêmicos e para a realização de estudos por órgãos de pesquisa**. Brasília, 2022. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/sei_00261-000810_20_22_17.pdf. Acesso em: 13 abr. 2023.
- BARROS, Bruno Mello Correa de; BARROS, Clarissa Teresinha Lovatto; OLIVEIRA, Rafael Santos de. **O direito à privacidade: uma reflexão acerca do anteprojeto de proteção de dados pessoais**. *Revista Lidere [recurso eletrônico]*, Dourados, MS, 2017, v. 9, n. 17, p. 13-27. Disponível em: https://ojs.ufgd.edu.br/index.php/videre/article/view/6029/pdf_1. Acesso em: 13 abr. 2023.
- BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 13 abr. 2023.
- BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei nº 10.973, de 2 de dezembro de 2004. Dispõe sobre incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo e dá outras providências**. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2004/lei/110.973.htm. Acesso em: 13 abr. 2023.
- BRASIL. **Estratégia Brasileira para a Transformação Digital**. 2018a. Disponível em: <https://www.gov.br/mcti/pt-br/centrais-de-conteudo/comunicados-mcti/estrategia-digital-brasileira/estrategiadigital.pdf>. Acesso em: 13 abr. 2023.
- BRASIL. Presidência da República. Casa Civil. Subchefia para Assuntos Jurídicos. **Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais**. 2018b. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm. Acesso em: 13 abr. 2023.
- BRASIL. Ministério da Economia. Comitê Central de Governança de Dados. **Guia de Boas Práticas - Lei Geral de Proteção de Dados Pessoais**. Brasília: Ministério da Economia, 2020. Disponível em: https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf. Acesso em: 25 abr. 2022.
- BRETTEL, Malte et al. **How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective**. *Journal of Information and Communication Engineering: World Academy of Science, Engineering and Technology International*, v. 8, n. 1, p.37-44, 2014. DOI: doi.org/10.5281/zenodo.1336426 Disponível em: <https://publications.waset.org/9997144/how-virtualization-decentralization-and-network-building-change-the-manufacturing-landscape-an-industry-40-perspective>. Acesso em: 13 abr. 2023.
- DONEDA, D. **A Proteção dos Dados Pessoais como um direito fundamental**. *Espaço Jurídico*, v. 12, n. 2, p. 91–108, 2011.
- FERREIRA, D. A. A.; PINHEIRO, M. M. K.; MARQUES, R. M. **Privacidade e proteção de dados pessoais: perspectiva histórica**. *InCID: Revista de Ciência da Informação e Documentação*, v. 12, n. 2, p. 151–172, 30 nov. 2021.
- INPI. Instituto Nacional de Propriedade Industrial. Rio de Janeiro, 2021. Disponível em: <https://www.gov.br/inpi/pt-br>. Acesso em: 13 abr. 2023.

MONTEIRO, J. R.; FÉLIX, V. **O uso de tecnologias e dados pessoais em políticas públicas de saúde no contexto da COVID-19.** *Civilistica.com*, v. 11, n. 1, p. 1-31, 2022.

PIRONTI, Rodrigo. ZILLOTTO, Mirela Miró. **O direito à autodeterminação informativa e a questão do consentimento no tratamento de dados pessoais pela administração pública.** In: PIRONTI, Rodrigo (coord.). *Lei Geral de Proteção de Dados no Setor Público*. Belo Horizonte: Fórum, 2021. p. 407-426.

RIBEIRO, Núbia Moura (org.). **Série Prospecção Tecnológica:** volume I. Salvador: IFBa, 2018. 192 p. (Coleção PROFNIT). Disponível em: <https://profnit.org.br/wp-content/uploads/2018/08/PROFNIT-Serie-Prospeccao-Tecnologica-Volume-1-1.pdf>. Acesso em: 13 abr. 2023.

UNIÃO EUROPEIA. Parlamento e Conselho europeus. **Regulamento (UE) 2016/679, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação destes dados e que revoga a Diretiva 95/46/CE.** União europeia, abr. 2016. Disponível em: <https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=EN>. Acesso em: 13 abr. 2023.

ZIMMERMANN, Alfred et al. **Architectural Decision Management for Digital Transformation of Products and Services.** *Complex Systems Informatics and Modeling Quarterly*, [s.l.], n. 6, p.31-53. 2016. Riga Technical University [recurso eletrônico]. Disponível em: <https://csimq-journals.rtu.lv/article/view/csimq.2016-6.03/816>. Acesso em: 13 abr. 2023.