Data Privacy in Educational Contexts: Analyzing Perceptions, Practices and Challenges in Personal Data Protection

Yuri Correia de Barros[a] and Jéssyka Vilela[b]
Centro de Informática, Universidade Federal de Pernambuco (UFPE), Av. Jornalista Aníbal Fernandes, s/n – Cidade Universitária, Recife-PE, Brazil
{*ycb, jffv*}*@cin.ufpe.br*

Keywords: Privacy, LGPD, Data Privacy, Educational Environment, Personal Data Protection, Systematic Mapping Study, Survey.

Abstract: This study aims to investigate the increasing relevance of data privacy in the educational context as digital processes and the use of technology become more prevalent in educational institutions. The protection of personal data, especially in academic environments, is a sensitive and challenging topic due to the large volume of information shared between students, teachers, and administrators, making the adoption of efficient and secure practices essential. The study analyzes current data security practices and the challenges faced by educational institutions in safeguarding personal information. Focusing on the guidelines and requirements established by data protection laws such as Brazil's LGPD and the European Union's GDPR, the research examines both the legal implications and ethical issues related to the treatment of personal data in the educational field. Alongside a detailed review of best practices and regulatory demands, the study is based on field research conducted through a survey with students and teachers from various institutions, including public universities, private institutions, and technical schools. The survey's goal is to understand users' perceptions of data protection and to assess their knowledge of the relevant legislation. This approach provides a critical insight into how prepared students and teachers are to address data privacy challenges in academic settings. The analysis of the research conducted with educators and students from educational institutions revealed key insights into the treatment of personal data. The results indicate concerns about transparency and data security, highlighting the need to improve education on privacy and promote more transparent practices within institutions, in line with the LGPD, to foster a safer and more ethical environment for students.

1 INTRODUCTION

Technology plays a crucial role in people's daily lives, and the collection and processing of personal data have become common practices. However, the growing concern about the privacy and security of this information highlights the importance of protecting it effectively and responsibly (Sá, 2022)(Santos et al., 2021).

It is essential to ensure students' privacy by preventing the unnecessary exposure of their personal data. This requires implementing clear internal policies about who can access such information and restricting sharing to authorized individuals only. Additionally, raising awareness among students, parents, and teachers about the importance of protecting personal data is critical. Providing clear guidelines on security practices in the digital environment can significantly enhance privacy protections (Sá, 2022)(Machado et al., 2023).

Cultural adaptation within institutions and among their employees regarding the need to handle personal data responsibly poses a considerable challenge (Santos et al., 2021). These changes require time and investment in adequate awareness programs and training. Integrating new data protection practices into the organizational routine demands ongoing efforts through regular training and educational campaigns (Rojas, 2020).

Educational institutions must commit to understanding the nuances of the LGPD (General Data Protection Law) and implementing policies that extend beyond IT. Engaging all staff members and students in this journey of awareness and accountability not only protects personal data but also fosters a safer and more ethical educational environment. Collaboration

[a] https://orcid.org/0009-0004-7490-2127
[b] https://orcid.org/0000-0002-5541-5188

Correia de Barros, Y. and Vilela, J.
Data Privacy in Educational Contexts: Analyzing Perceptions, Practices and Challenges in Personal Data Protection.
DOI: 10.5220/0013426900003929

In *Proceedings of the 27th International Conference on Enterprise Information Systems (ICEIS 2025) - Volume 2*, pages 308-319
ISBN: 978-989-758-749-8; ISSN: 2184-4992

among all stakeholders is essential to cultivate a culture of respect for privacy and information security, ensuring everyone is aware of and responsible for adhering to data protection laws and guidelines (Martirena, 2022).

The collection of personal data is a common practice in universities, starting during the enrollment process when students provide personal information and documents. This data circulates across various institutional departments, including academic offices and administrative areas.

In addition to personal information, higher education institutions also access financial data such as financing contracts, bank details, and family income. Furthermore, academic performance and students' histories throughout their courses are also recorded (Rosso, 2023).

In the digital era, information is a valuable resource, and data protection has become a necessity. This need has led to the emergence of new legislation worldwide to regulate data use and processing. A notable example is the General Data Protection Regulation (GDPR), effective since 2018 in the European Union, which inspired the creation of Brazil's LGPD (de Lucena et al., 2024).

The improper disposal of documents containing personal data poses serious risks to individuals. Information such as names, addresses, grades, and academic records can be exploited by criminals for fraud, identity theft, reputation damage, and other offenses (Mackenzie,).

Each sector has specific characteristics that deserve consideration. In the educational context, the inherent nature of education—focused on culture dissemination, learning, and training—facilitates the promotion of data protection rules, primarily involving teachers and students (SERPRO, 2020).

Against this backdrop, it is essential to analyze how students and teachers understand the collection and processing of their data under the LGPD. This study aims to address this through a survey applied to educational institutions and a systematic literature review.

This study's primary objective is to analyze the various types of personal data collected in educational institutions and the main problems and challenges related to data protection in these settings. By exploring the complexity of personal data in this context, the research seeks to understand which information is collected, processed, and utilized within educational environments. Furthermore, it aims to highlight the growing importance of personal data protection in the educational community.

Ultimately, the research seeks to understand how users perceive data protection and assess their level of knowledge about current legislation in educational environments. This analysis will provide a critical perspective to answer the following research question: *How are personal data collected, processed, and protected in educational institutions, and what challenges and practices are associated with their use?*

This document is organized as follows: Section 2 presents the main concepts addressed in this study; Section 3 describes the research methods employed; Section 4 discusses the findings; and finally, Section 5 outlines the conclusions and suggestions for future research.

2 BACKGROUND AND RELATED WORK

2.1 LGPD

The General Data Protection Law (LGPD) was inspired by the European Union's General Data Protection Regulation (GDPR), a regulation focused on privacy and data protection. In Brazil, the protection of personal data has been recognized as a fundamental right, ensuring the right to data protection, including in digital media, as established by law. The LGPD aligns with the latest international standards for personal data protection. It was created to regulate the use of citizens' information, including in digital media, ensuring the rights to privacy, freedom, and personal development. It applies to any individual or organization, public or private, that processes personal data, whether online or offline (GOVERNO DO ESTADO DE RONDÔNIA, 2023). This means that every individual has the right to decide how their personal data will be used by others, including companies and government entities.

The LGPD outlines its main principles for personal data protection in Article 2. These principles include respect for privacy, ensuring fundamental rights such as the inviolability of intimacy, honor, and private life. Another crucial aspect is informational self-determination, which grants citizens control over their data. The law also protects freedom of expression, information, and opinion while promoting economic and technological development by fostering a legally secure environment. Additionally, the LGPD reinforces free enterprise, fair competition, and consumer protection while safeguarding human rights, dignity, and citizenship (BRASIL, 2018).

Thus, the LGPD aims to balance the protection of fundamental rights by modernizing and clarifying concepts to minimize risks and establish clear rules

for the processing of personal data (Maldonado and (Coord.), 2020).

The LGPD sets essential rules for personal data use, ensuring security and respect for privacy. Data must be processed for legitimate and specific purposes, as informed to the data subject. Only necessary information should be used, and individuals have the right to easy and free access to information about their data. The data must be accurate and up to date, and processing must be transparent, providing clear information about how and by whom the data is used. Security measures must be adopted to prevent unauthorized access or issues such as loss and alterations. The LGPD also prohibits data use for discriminatory purposes, requiring accountability and compliance from those processing the data.

2.2 Educational Environment

The term ”educational environment” is used in various contexts and can seem broad. Generally, it refers to any context where teaching and learning processes occur. It can also be described as the ”educational context” or ”educational space.”

The educational environment not only influences the quality of education but also determines the success of learning outcomes. An essential aspect of this definition is the active role of the student, who is not merely a recipient but also a participant in the environment, taking part in its maintenance and improvement. Thus, the educational environment includes not only the infrastructure and resources provided by the institution but also the human interactions and emotional conditions that directly impact educational development (de A. Troncon, 2014).

2.3 Related Works

(Baloyi and Kotzé, 2017) conducted an investigation through a survey into the perceptions and practices of individuals in South Africa regarding the use of their personal information. The study aimed to understand privacy concerns, knowledge levels about legal rights, and risks associated with data sharing. Using a 12-question ”yes” or ”no” questionnaire with snowball sampling, the research gathered 138 responses from diverse professional fields such as healthcare, telecommunications, and information technology. Key findings revealed that 79% of participants do not read privacy policies, highlighting a tendency to prioritize convenience over data security. Despite this, nearly 80% recognized the dangers of data misuse, while 20.3% did not share this perception. Furthermore, nearly 72% of respondents expressed distrust in organizations’ ability to protect their data, indicating that transparency and security practices are not yet deemed reliable. The study concludes that, although awareness of privacy importance is growing, many South Africans are unaware of their legal rights and underestimate the risks of data misuse. The article recommends educational campaigns and increased transparency from organizations to build trust and enhance personal data security.

(Martinovic and Ralevich, 2007a) discuss the complexity of privacy in educational systems, emphasizing its growing relevance as digital technology expands. They argue that educational institutions face challenges in managing students’ personal data, particularly on online platforms, and stress the need for a comprehensive approach to handle this data securely and ethically. The authors highlight that privacy concepts vary by cultural and political context, citing examples from the United States, where privacy focuses on individual freedom; the European Union, which prioritizes human dignity; and Canada, where there is a balance between concerns over government surveillance and private sector misuse. They analyzed types of personal data collected by educational institutions, such as student identities, academic performance, and demographic data, highlighting risks associated with improper handling. They also explored data security practices like partial encryption and two-step access controls, which may be insufficient for guaranteeing data security. The study underscores the lack of awareness among users, including students and teachers, about data security practices and calls for greater transparency and rigorous institutional practices to ensure privacy protection.

(Mollick and Pearson, 2003) investigated how students’ concerns about the collection and use of their personal data by universities influence their sense of ”alienation.” Conducted with 187 students from a U.S. university, the study used a questionnaire to assess the impact of these concerns. The authors identified two main concerns: data collection and data use. Lack of transparency in institutional data collection practices emerged as a significant factor contributing to distrust. Students felt inadequately informed about how their information was collected and used, leading to feelings of insecurity. The study also revealed that concerns over the collection of sensitive data, such as race and sexual orientation, were strongly linked to alienation. The findings suggest that universities need to be more transparent about their data practices to reduce student concerns and improve trust.

(E. Mougiakou and Virvou, 2020) focused on compliance of educational platforms with the General Data Protection Regulation (GDPR). They high-

lighted the need for educational practices to respect students' rights and privacy. The study identified challenges faced by educational institutions in implementing synchronous and asynchronous learning platforms. One key finding was that lack of clarity in data collection and usage could infringe on user rights, such as the "Right to be Informed" and the "Right to Object," as stipulated by the GDPR. The authors proposed practical suggestions for designing GDPR-compliant educational platforms, including conducting Data Protection Impact Assessments (DPIAs) before data processing and clearly communicating user rights. They emphasized the importance of education and awareness among students and stakeholders regarding data privacy risks. By ensuring ethical and responsible handling of student data, institutions can improve learning experiences and foster trust.

The comparison presented in Table 1 highlights the methodologies, participants, privacy laws, and conclusions of several related studies, alongside the current research. Each study contributes unique insights into privacy and data protection across different contexts, illustrating diverse approaches and outcomes.

Table 1: Comparison of Related Works and our Study.

Authors	Method	#d	Privacy Law	Conclusion
N. Baloyi and P. Kotzé (2017)	Survey	138	POPI and PAI	Actions and recommendations to enhance awareness and protection of personal data in South Africa.
Mollick J.S. and Pearson J.M. (2003)	Survey	187	USA	Recommendations for improving privacy practices in universities.
Martinovic D. and Ralevich V. (2007)	Data Model Comparison	Not Applicable	Various (USA, Canada, EU)	Critical analysis of privacy issues in educational systems, highlighting the importance of regulations.
E. Mougiakou et al. (2020)	Review of Practices	Not Applicable	GDPR	Guidelines for managing personal data in educational institutions, with a focus on GDPR compliance.
This Study (2024)	Survey	125	LGPD	Analyze students' and teachers' perceptions of personal data protection in educational environments.

3 RESEARCH METHOD

The study utilized the survey and systematic review methodologies due to their effectiveness in collecting and analyzing data consistently. The research steps conducted in each method are described in the next sections.

3.1 Survey

Following the framework by (Kasunic, 2005), the survey aimed to gather insights into user perceptions of data privacy and LGPD compliance in educational settings. The survey aimed to answer the Survey Research Questions (SURQ) listed in the first column of Table 2.

The survey was conducted following five steps.

Definition and Objectives: The research defined its goals through preliminary studies focusing on data privacy culture, legislation, and user understanding. This informed the research direction to address the challenges in educational contexts.

Target Audience: The participants included professors and students from public, private, and technical higher education institutions. The aim was to capture a comprehensive understanding of their knowledge and concerns about data handling.

Questionnaire Design: A structured questionnaire was developed, starting with general questions and moving toward more specific ones. It comprised 4 common profile questions for all participants and 10 tailored questions for students and professors, along with one open-ended question for each group. Google Forms was used for its accessibility and reach. The questions are listed in the second column of Table 2.

Pilot Test: A pilot test with two participants ensured clarity and improved question phrasing. The survey duration averaged 5 minutes, balancing comprehensiveness and participant engagement.

Distribution: The questionnaire was distributed via institutional emails and social media platforms such as WhatsApp and Instagram from August 6 to September 21, 2024, encouraging voluntary participation and further sharing.

Response Analysis: The survey received 125 responses (17 professors, 108 students) with a total of 15 open-ended comments. The data provided insights into participants' perceptions of privacy and their knowledge of LGPD.

The analyses obtained from the results are presented in Section 4 of this work. The application of the survey allowed for collecting volunteers' general impressions regarding privacy and security, as well as evaluating their level of knowledge about the General

Table 2: Mapping of Survey Research Questions to Survey Questions.

Survey Research Question	Survey Questions
SURQ1. What is the level of knowledge of students and teachers about regulations and practices for personal data protection in the educational environment?	• How do you evaluate your knowledge of your privacy rights? • How do you evaluate your knowledge about the General Data Protection Law (LGPD)? • Do you know how to request the correction or deletion of your personal data at the educational institution? • Do you know whom to contact at the institution regarding data protection issues?
SURQ2. What practices and policies are perceived by participants regarding the collection, processing, protection, and transparency of personal data?	**For teachers:** • Did the institution provide training on LGPD? • Are you aware of the privacy policies? • Do you know how to protect students' personal data? • Are the collected data secure? • Is the data processing ethical? • Is the data processing transparent? **For students:** • Do you have easy access to privacy policies? • Is consent requested clearly and explicitly? • Are students' personal data secure?
SURQ3. What are the main concerns, challenges, and perceptions about personal data processing in educational institutions?	**For teachers:** • Have you processed students' personal data? • What personal data have you processed? • Have you dealt with data protection-related issues? **For students:** • How concerned are you about data protection? • Have you experienced or know someone who has experienced data misuse or leaks? • What data do you believe the institution collects?

Data Protection Law within the educational environment.

3.1.1 Threats to Validity

When designing a survey, it is essential to be aware of threats to validity, as they can compromise the accuracy of the results obtained. Two main types of validity were considered: construct validity, which evaluates whether the questionnaire truly measures what it is intended to measure, and external validity, which examines to what extent the results can be applied to different groups, contexts, or time periods.

To minimize these threats, the survey was carefully designed, aligning each question with the research objectives. Through a pilot test, the survey was structured to avoid ambiguous interpretations, with a clear order of questions. Additionally, the total response time was planned to be concise, to avoid demotivation or rushed and uninterested answers. The questionnaire was distributed to students and teachers from various fields and higher education institutions, including public, private, and technical universities, encompassing a diversity of profiles and experiences. Furthermore, the survey was disseminated at two different points during the academic period to ensure that the responses were not influenced by a specific moment.

3.2 Systematic Literature Review

A Systematic Literature Review (SLR) was conducted following the guidelines outlined by (Kitchenham et al., 2009) to systematically collect and analyze relevant data on personal data processing in the educational environment.

3.2.1 Planning the Review

To effectively design the SLR, it was essential to develop research questions to guide the search and selection processes. Therefore, the central research question (*How are personal data collected, processed, and protected in educational institutions, and what challenges and practices are associated with their use?*) was expanded into the following secondary questions:

- Q1 - What are the most common problems and challenges related to personal data protection faced by teachers and students in educational institutions?
- Q2 - What are the main practices adopted by educational institutions to ensure compliance with GDPR/LGPD in personal data processing?
- Q3 - What personal data is handled by educational institutions?
- Q4 - What type of data processing is carried out?

To thoroughly address these research questions, a comprehensive search string was designed to capture the core concepts and ensure the focused and extensive retrieval of relevant literature. The search string integrates the key terms ""personal data processing" and "educational" context resulting in the following search string:

("personal data processing" OR "personal data handling" OR "personal data storage" OR "personal

data collection" OR "subject data processing" OR "subject data handling" OR "subject data storage" OR "subject data collection") AND ("educational" OR "educational institution" OR "high school" OR "university").

3.3 Conducting the Review

The research methodology adopted for this study included an automated search performed across five leading academic databases: IEEE, Science Direct, ACM, Scopus, and SOL (SBC Open Lib)[1].

In the initial search, 126 results were obtained across the five databases: IEEE (80 articles), Science Direct (3 articles), ACM (4 articles), Scopus (39 articles), and no articles were returned from SOL.

A systematic three-step selection process was employed to select the relevant studies. In the first step, a pre-selection process applied exclusion criteria based solely on the abstract. These criteria included studies that were unavailable for access, required payment, were duplicates, fell outside the defined research area, were early access articles, or had fewer than four pages.

The second step implemented inclusion criteria to refine the selection further. These criteria were as follows: (1) articles published between 2018 and 2023, (2) articles written in English or Portuguese, (3) studies within the field of computer science or related disciplines, and (4) publications categorized as journal articles, conference papers, or similar scholarly works. After filtering based on the title and abstract, 110 articles remained, with an additional 18 articles approved after analyzing their introduction and conclusion sections, resulting in a total of 17 articles.

In the final step, quality criteria were applied to evaluate each study. These criteria used were *"clear context," "well-defined methodology," "practical application," "relevant and consistent discussion,"* and *"limitations and threats of the research addressed."* A grading system was used, assigning scores of 0, 0.5, or 1 for each criterion, with a maximum possible score of 5 points per study. Studies scoring below 2.5 points were excluded, and any article scoring zero in the "Answers at least one research question" criterion was also discarded. Ultimately, 6 papers, listed in Table 3, were selected to data extraction.

3.3.1 Threats to Validity

The primary threat to validity in the systematic review was the difficulty in finding articles within the restricted scope of the research, which specifically focused on the educational context and its relation to LGPD. Most of the identified articles addressed data protection in broader scopes, complicating the acquisition of materials that dealt specifically with educational environment dynamics. Only one directly related article was identified, which limited the scope of the conclusions.

Moreover, challenges arose in constructing the search string. The limitations imposed by connectors in Science Direct, where only eight connectors were allowed, may have restricted more satisfactory results. To address this issue, the search string was adjusted to include terms more focused on the central theme, but the limitation of specific articles persisted.

Table 3: Selected Papers on Data Privacy in Educational Contexts.

ID	Title	Authors	Citation
S1	Synchronous and Asynchronous Learning Methods under the light of General Data Protection Regulation	E. Mougiakou; S. Papadimitriou; M. Virvou	(Mougiakou et al., 2020)
S2	Do users know or care about what is done with their personal data: A South African study	N. Baloyi; P. Kotzé	(Baloyi and Kotzé, 2017)
S3	Towards automated personalized data storage	J. Lange; A. Labrinidis; P. K. Chrysanthis	(Lange et al., 2014)
S4	Effects of Two Information Privacy Concerns on Students' Feeling of Alienation	Mollick J.S.; Pearson J.M.	(Mollick and Pearson, 2003)
S5	Personal Learning Environments as socio-technical systems: does decentralised data finally give us the right balance	Rajagopal K.	(Rajagopal, 2023)
S6	Privacy issues in educational systems	Martinovic D.; Ralevich V.	(Martinovic and Ralevich, 2007b)

4 RESULTS

4.1 Survey Results

4.1.1 Subjects' Profile

The participant profile reveals two distinct groups: professors and students. Among students, 67% fall within the 18-25 age range, indicating a concentration of young adults, followed by participants aged 26-35. For professors, the age distribution is more balanced, with the highest proportion in the 46-55 age

[1]https://sol.sbc.org.br/index.php/indice

range, followed by equal representation in the 26-35 and 36-45 brackets, and a smaller group over 55 years old. Most participants (96%) are affiliated with public universities, likely due to the institutional email channels used for recruitment. Additionally, 86.4% of respondents are students, emphasizing the study's strong focus on this group.

4.1.2 Level of Knowledge About User Rights Under LGPD

There are notable differences in the distribution of responses regarding the level of knowledge students and professors have about the General Data Protection Law (LGPD), particularly at the extremes of "very little" and "very good." Among students, only 1.9% claimed to have a very good understanding, while 34.3% reported very limited knowledge. Professors demonstrated similar patterns, with 5.9% evaluating their knowledge as very good and 11.8% as very little. Most participants, however, fell within the "moderate" and "low" categories, with 58.8% of professors and 55.6% of students indicating intermediate levels of knowledge. Additionally, professors were slightly more likely to rate their knowledge as "good," suggesting a somewhat stronger understanding of LGPD among faculty. Figure 1 illustrates these findings.

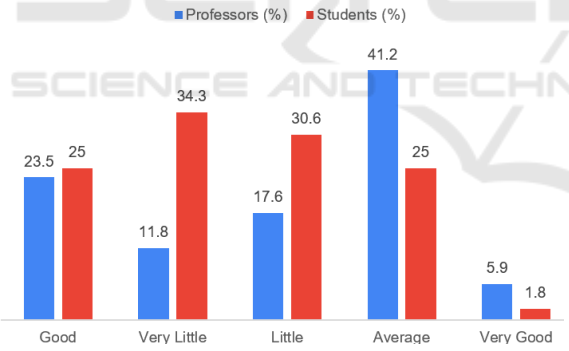

Figure 1: Perception of Knowledge about LGPD by Professors and Students.

4.1.3 Professors' Perception of Personal Data Handling in Educational Institutions

Regarding the **courses in which the professors teach**, the majority, 58.8%, selected "Other" as their course category, suggesting a variety of disciplines not explicitly listed. "Computer Science" follows with 52.9%, and "Information Systems" with 17.6%. Additional courses, including "Biomedical Sciences," "Medicine," and "Computer Engineering," were represented by 5.9% each. No responses were recorded for the remaining listed courses, such as Administration, Social Sciences, Law, Mathematics, and others. This distribution highlights a predominance of respondents involved in diverse and technology-related disciplines.

Most professors (58.8%) reported that t**heir institutions did not offer training or guidance on LGPD**, with 29.4% having received some training and 11.8% unsure (Figure 7). Regarding awareness of privacy and data protection policies, 76.5% of professors were unaware, with 11.8% either aware or unsure.

When asked about **knowledge of procedures to protect students' personal data**, 64.7% of professors reported being unaware of such procedures, compared to 29.4% who were informed and 6% who were uncertain.Regarding **trust in the institution's data storage security**, 47% believed the data was secure, while 29.4% were unsure, and 23.5% disagreed.

Ethical concerns about data collection and handling revealed that 64.7% of professors believed the practices were ethical, 29.4% were unsure, and 5.9% disagreed.Transparency during data collection was also a concern, with 41.2% unsure, 35.3% agreeing it was transparent, and 23.5

Regarding **experience with personal data handling**, presented in Figure 2, 47.1% of professors had performed data-related activities, while 35.3% had not, and 17.6% were unsure.The most commonly handled data types were names (58.8%), enrollment numbers (47.1%), and CPF numbers (a unique Brazilian taxpayer registry number - 29.4%). Other data types, such as ethnic origin and health data, were handled by smaller proportions, while some categories, such as religious beliefs and political opinions, were not handled at all.

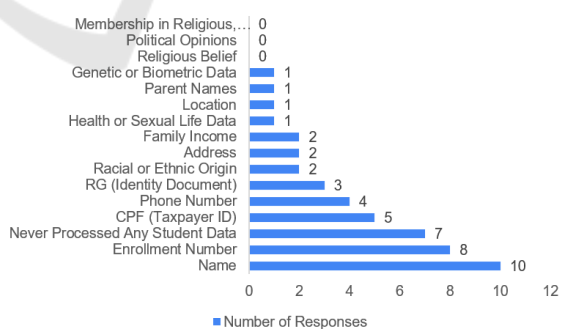

Figure 2: Types of Student Personal Data Processed by Respondents.

Notably, **none of the professors reported encountering issues related to personal data protection involving students**.A single participant expressed concern in an open-ended question, stating they lacked knowledge on the subject.

4.1.4 Students' Perception of Personal Data Handling in Educational Institutions

Regarding the **courses in which students are enrolled**, 30.6% selected "Other," indicating a variety of disciplines not explicitly listed. "Computer Science" follows closely with 28.7%, while "Dentistry" accounts for 12%. "Information Systems" represents 11.1%, and "Computer Engineering" and "Physiotherapy" each account for 8.3%. "Psychology" was the least represented, with 1% of responses. This distribution highlights a significant representation of technology-related courses, while also reflecting diversity among other disciplines.

Students expressed significant concerns about data privacy, with 60% worried about protecting personal information, 56% concerned about sharing data with online companies, and 46% about sharing with offline entities. Only 3% reported no concern across all topics (Figure 3). Regarding knowledge of privacy rights, most students reported low levels of awareness, with only 8.3% indicating good knowledge and 1.8% very good knowledge.

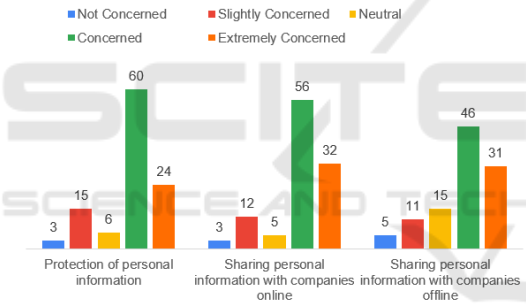

Figure 3: Levels of Concern Regarding Personal Information.

When asked if **they knew someone affected by improper data usage or leaks**, 62% responded affirmatively, 28.7% negatively, and 9.3% were unsure. Students also identified common data types collected by institutions, including CPF (99.07%), RG (94.44%), phone numbers (93.52%), and enrollment numbers (91.67%). Less frequently mentioned categories included religious beliefs (9.26%) and political affiliations (4.63%) as presented in Figure 4.

Regarding **access to privacy policies**, 51% were unsure, 44.5% found access difficult, and only 4.5% found it easy.Similarly, 83% of students were unaware of how to request data correction or deletion, with only 11.1% knowing the process.

Students were divided on whether **their data was secure with the institution**: 38% disagreed, 32.5% were unsure, and 30% agreed.Transparency regarding consent for data collection and sharing was also

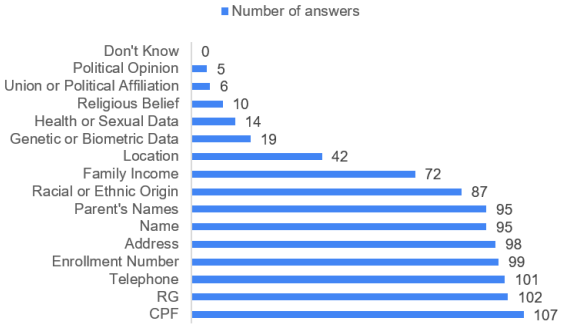

Figure 4: Levels of Concern Regarding Personal Information.

questioned, with 42.6% unsure, 37% disagreeing, and 20.4% agreeing.Lastly, 78% of students did not know whom to contact for data-related issues, with only 15.7% aware of the appropriate channels.

4.1.5 Summary of the Survey Research Questions

SRQ1: What is the level of knowledge of students and teachers about regulations and practices for personal data protection in the educational environment?

The study found that both students and teachers exhibit limited knowledge regarding the General Data Protection Law (LGPD) and their privacy rights. Among students, only 1.9% reported having a "very good" understanding, while 34.3% admitted to having "very little" knowledge. Professors showed slightly better awareness, with 5.9% rating their knowledge as "very good" and 11.8% as "very little." Most participants fell within the "moderate" or "low" categories, with 58.8% of professors and 55.6% of students indicating intermediate levels of knowledge. This demonstrates a significant gap in awareness and highlights the need for educational initiatives. Moreover, many professors noted the absence of institutional training on data protection laws, with 58.8% confirming they had not received any training. These results emphasize that both students and teachers are inadequately prepared to address data privacy challenges in educational environments.

SRQ2: What practices and policies are perceived by participants regarding the collection, processing, protection, and transparency of personal data?

The study revealed several concerns and deficiencies in institutional practices and policies related to personal data handling. Among professors, 76.5% were unaware of their institution's privacy policies, and 64.7% did not know how to protect student data. Only 47% of professors believed that the collected data was securely stored, and 35.3% considered the data collection process transparent. Training gaps

were evident, with nearly 59% of professors stating they had not received guidance on the LGPD.

Students, on the other hand, struggled with accessing privacy policies, with 51% unsure about how to find them and 44.5% finding access difficult. Transparency issues were also a concern, as 42.6% of students were unsure whether consent for data collection was explicitly requested, and 37% disagreed entirely. Regarding the security of personal data, 38% of students believed their data was not secure, compared to 30% who thought it was secure. These findings reflect a systemic lack of communication and transparency between institutions and their members.

SRQ3: What are the main concerns, challenges, and perceptions about personal data processing in educational institutions?

Both students and teachers expressed significant concerns about the handling of personal data in educational settings. For students, key challenges included a lack of transparency about what data was collected and how it was used, as well as fears about data misuse. Notably, 62% of students knew someone who had experienced a data breach or improper data usage. Students also expressed high levels of concern about data sharing with online companies (56%) and offline entities (46%).

Professors reported handling various types of student data, including names (58.8%), enrollment numbers (47.1%), and CPF (29.4%). However, many professors (64.7%) were unaware of proper procedures for safeguarding student data, highlighting a gap in institutional support and training. Furthermore, ethical concerns were raised, with 29.4% of professors unsure whether their data handling practices were ethical.

The study underscores the need for robust institutional measures to address these concerns, such as clearer privacy policies, enhanced training programs, and the promotion of transparency in data collection and processing practices.

4.2 Results of the Systematic Literature Review

RQ1: What are the most common problems and challenges related to personal data protection faced by teachers and students in educational institutions?

- Lack of transparency in data collection: Failing to inform users about the data being collected conflicts with the right to be informed, as established by the GDPR. This issue is common in educational platforms, which often do not clearly disclose what information is being stored or used (Mougiakou et al., 2020).
- Lack of awareness of legal rights: While not specifically addressing educational institutions, (Baloyi and Kotzé, 2017) identified the lack of knowledge about data collection and processing rights as a critical challenge. Only 45.7% of respondents were aware of their legal rights, leaving a significant number of individuals without adequate information to protect their data.
- Concerns about data usage: Students expressed concerns during interviews, highlighting that they are not adequately informed about how universities use the data they collect. This lack of clarity fosters insecurity about the handling of personal information (Mollick and Pearson, 2003).
- Skepticism about institutions' use of data: Teachers and students display distrust regarding how educational institutions use their personal data (Rajagopal, 2023).
- Difficulty understanding data security: Even among those with technological knowledge, many still struggle to comprehend the importance of data security and how to ensure privacy in digital environments. This indicates a significant gap in education about privacy and data protection (Martinovic and Ralevich, 2007b).

RQ2: What are the main practices adopted by educational institutions to ensure compliance with GDPR/LGPD in personal data processing?

Use of two-factor access controls and data encryption: However, the article mentions that these measures are insufficient to adequately protect sensitive data and ensure individual privacy (Mackenzie,).

RQ3: What personal data is handled by educational institutions?

According to the work of (Mackenzie,), educational institutions using the SAM Learning platform collect and handle various personal data from students. These include first name, last name, enrollment number, gender, date of birth, registration group, academic year, classes, and enrollment. Additionally, according to (Mougiakou et al., 2020), the Intelligent Tutoring System (ITS) collects and processes student data using advanced techniques. When students choose to participate in the system's exercises, they must create an account, granting the platform access to their email. However, it is not explicitly specified what other data is collected by the platform.

RQ4: What type of data processing is carried out?

The processing involves collecting, storing, and processing data to generate progress reports, create login IDs, track students' academic development, and produce statistical reports. Additionally, the data ensures that students' information remains complete and

up-to-date, especially in cases of transfer. This processing serves both administrative and educational purposes (Mackenzie,).

4.3 Discussion

The survey conducted with professors and students from educational institutions revealed significant insights into their perceptions and knowledge regarding personal data handling. The sample was predominantly composed of young adults aged 18 to 25 (58% of all respondents), indicating a strong concentration of students in their early stages of education. Additionally, most participants (96%) were affiliated with public universities, which may limit the generalizability of results to other types of institutions that could have different approaches to handling personal information.

Regarding participant profiles, 86.4% were students, while professors represented 13.6%. Despite the smaller proportion of faculty, their participation was notable compared to recent university data (2022), indicating that professors comprise approximately 7% of the academic community. The survey's 13.6% faculty representation thus nearly doubles the institutional average, reflecting strong engagement with the topic and enriching the diversity of perspectives analyzed.

Data Security Perception and Awareness. Comparing the data security perceptions of professors and students reveals shared concerns. While 47% of professors believe student data is secure, only 29.6% of students share this view. This discrepancy suggests insecurity among students and highlights a potential weakness in implementing robust information security policies. Both groups' significant lack of trust indicates the urgent need for institutions to review and strengthen their security practices to ensure LGPD compliance and build trust among stakeholders (Figure 5).

Awareness of Privacy Policies Also Reveals Critical Issues. While 76.5% of professors reported being unaware of these policies, 44.5% of students reported difficulty accessing them, and 51% were unsure. This lack of transparency contradicts LGPD principles and undermines trust between institutions and their members. Transparency and Training

The **transparency of data collection processes** was also concerning. Only 35.3% of professors considered data collection transparent, while 42.6% of students were unsure if consent was obtained explicitly and 37% disagreed entirely. The absence of clear informed consent processes jeopardizes the integrity of data collection practices and may further erode trust.

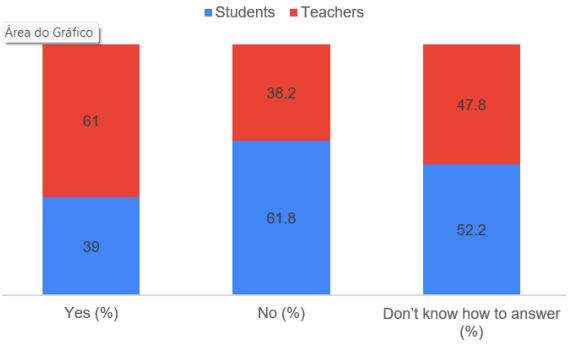

Figure 5: Comparison (normalized percentage) between Students and Teachers regarding the perception of the security of students' personal data at the educational institution.

Training Deficiencies Exacerbate the Issue. Nearly 58.8% of professors had no training or guidance on LGPD, and most students assessed their knowledge as "very limited" (34.3%) or "low" (30.6%). This correlation suggests that insufficient faculty training may directly impact students' awareness of personal data protection.

Data Handling and Concerns. Both groups identified "name," "enrollment number," "CPF," and "phone number" as the most commonly handled or collected data. Among professors, "name" was the most handled (59%), while 88% of students believed it was collected. However, students' perception that "CPF" is frequently collected (99.07%) contrasts with professors' practices, where only 30% reported handling this data. This disparity might arise from students associating CPF usage with academic identification.

Concerns about data sharing with online companies were most pronounced, with 32% of students expressing extreme concern. This reflects widespread distrust of digital platforms.

Finally, the survey highlighted significant g**aps in understanding data protection procedures**. More than 64.7% of professors did not know how to safeguard student data in academic activities, and 83% of students did not know how to request data correction or deletion, underscoring institutional failures in providing clarity.

Open-Ended Responses Highlighted Growing Concerns About Data Protection in Educational Settings. Participants emphasized issues like improper use of sensitive information, such as CPF, and a lack of transparency in data storage and management. Some expressed interest in understanding how data is stored, revealing a demand for greater transparency and accessibility of privacy policies. These reflections underscore the need for robust measures

to ensure LGPD compliance and data security for all stakeholders.

5 CONCLUSIONS AND FUTURE WORK

Currently, technology plays an essential role in people's daily lives, and the collection and processing of personal data have become common practices. However, growing concerns about privacy and information security emphasize the importance of protecting such data effectively and responsibly [1].

It is crucial to ensure student privacy by avoiding the unnecessary exposure of their personal data. This requires well-defined internal policies regarding who can access such information and limiting its sharing to authorized individuals only. Moreover, raising awareness among students, parents, and teachers about the importance of protecting personal data is vital. Institutions should provide clear guidance on how to act safely in digital environments [1].

Adapting an institution and its staff to the necessity of processing personal data is a considerable challenge, as such transformations require time and investments in adequate awareness and training programs. These changes do not happen quickly and demand ongoing efforts, such as regular training sessions and educational campaigns, to integrate new data protection practices into organizational routines [2, p. 20].

Educational institutions must commit to understanding the nuances of LGPD (General Data Protection Law) and implementing policies that go beyond information technology. By engaging all professionals and students in this journey of awareness and responsibility, institutions not only protect personal data but also foster a safer and more ethical educational environment. Collaboration among stakeholders is fundamental to cultivating a culture of respect for privacy and information security, ensuring that everyone is aware of and accountable for compliance with data protection laws and guidelines [3, pp. 77-78].

5.1 Research Contributions

This research on personal data protection in educational settings provides valuable insights into the gaps and challenges in this context. It sheds light on how teachers and students deal with privacy and the management of their personal information.

One of the main contributions is the urgent need for training and awareness. The survey revealed that many stakeholders are unaware of proper procedures for protecting their data or requesting corrections or deletions, highlighting a critical area for improvement by institutions. This finding reinforces the importance of educational initiatives to enhance understanding of privacy-related rights and responsibilities.

Another important point is the growing distrust regarding data sharing. The lack of transparency and perceived insecurity in data handling jeopardizes trust among students, teachers, and institutions. Survey results, combined with findings from related studies, underscore the need for more ethical and secure data-handling practices.

The study also highlights that although educational institutions collect and store vast amounts of data, many users do not fully understand how this information is processed. This calls for more transparent and accessible communication, ensuring that all stakeholders have clarity about the use of their data.

There are very few studies that focus on how personal data is handled in educational institutions, which makes it harder to improve understanding and create effective practices in this area. From the analysis, only six articles met the inclusion criteria, showing a clear gap in research that connects data protection laws, like the LGPD, with the reality of schools and universities. This lack of studies highlights the need for more research to better understand the challenges these institutions face, such as following legal rules, dealing with ethical issues, and finding solutions that fit their specific needs. Increasing research on this topic is important to create safer and more transparent ways of handling personal data, helping students, teachers, and administrators feel more confident and informed.

These contributions are essential for building a safer, more transparent educational environment aligned with LGPD requirements, promoting more ethical and secure personal data handling practices.

5.2 Future Work

To expand and deepen research on personal data protection in educational settings, several future directions can be pursued. Firstly, conducting more detailed studies to identify the main difficulties faced by educational institutions in implementing LGPD would be valuable.

Expanding research to include data from different educational levels, such as elementary and technical schools, and more diverse profiles among stakeholders would allow a more comprehensive analysis of how data protection is addressed in varied educational contexts.

Additionally, developing and testing technologi-

cal solutions that facilitate compliance with data protection regulations, such as automated consent management tools and personal information management systems, would be beneficial. Conducting longitudinal studies to evaluate the impact of data protection practices over time, particularly regarding the trust that students and teachers place in institutions, is another promising avenue.

Finally, exploring how data protection policies influence students' academic experiences by analyzing the impact of data collection and processing on their perception of privacy and security in educational institutions could provide valuable insights.

ACKNOWLEDGEMENTS

We would like to thank all subjects that participated in the study.

REFERENCES

Baloyi, N. and Kotzé, P. (2017). Do users know or care about what is done with their personal data: A south african study. In *2017 IST-Africa Week Conference (IST-Africa)*, pages 1–11. IEEE.

BRASIL (2018). Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Accessed: 2024-09-09.

de A. Troncon, L. E. (2014). Ambiente educacional. *Medicina (Ribeirão Preto)*, 47(3):264–271. Accessed: 2024-10-08.

de Lucena, B. A., Neves, I. V. B. W., de Alcântara, J. B., Camarago, M. E., and Neto, A. T. M. (2024). Systematic review in the implementation of the general data protection law in brazil. *Multidisciplinary studies: management and legal Sciences*, page 20.

E. Mougiakou, S. P. and Virvou, M. (2020). Synchronous and asynchronous learning methods under the light of general data protection regulation. In *2020 11th International Conference on Information, Intelligence, Systems and Applications (IISA)*, pages 1–7, Piraeus, Greece.

GOVERNO DO ESTADO DE RONDÔNIA (2023). Cartilha da Lei Geral de Proteção de Dados Pessoais (LGPD). Accessed: 2024-09-23.

Kasunic, M. (2005). Designing an effective survey.

Kitchenham, B., Brereton, O. P., Budgen, D., Turner, M., Bailey, J., and Linkman, S. (2009). Systematic literature reviews in software engineering–a systematic literature review. *Information and software technology*, 51(1):7–15.

Lange, J., Labrinidis, A., and Chrysanthis, P. K. (2014). Towards automated personalized data storage. In *2014 IEEE 30th International Conference on Data Engineering Workshops*, pages 278–283. IEEE.

Machado, P., Vilela, J., Peixoto, M., and Silva, C. (2023). A systematic study on the impact of gdpr compliance on organizations. In *Proceedings of the XIX Brazilian Symposium on Information Systems*, pages 435–442.

Mackenzie. A importância da segurança no descarte de material contendo dados pessoais.

Maldonado, V. N. and (Coord.), R. O. B. (2020). *LGPD: Lei Geral de Proteção de Dados comentada [e-book]*. Thomson Reuters Brasil, São Paulo, 2nd ed., revised, updated, and expanded edition. Various authors, Bibliography.

Martinovic, D. and Ralevich, V. (2007a). Privacy issues in educational systems. *International Journal of Information and Technology Systems*, 4(2):132–150.

Martinovic, D. and Ralevich, V. (2007b). Privacy issues in educational systems. *International Journal of Internet Technology and Secured Transactions*, 1(1-2):132–150.

Martirena, R. P. (2022). A proteção de dados pessoais e da propriedade intelectual no ensino remoto: estudo de caso no centro universitário uniprojeÇÃo.

Mollick, J. and Pearson, J. (2003). Effects of two information privacy concerns on students' feeling of alienation. *AMCIS 2003 Proceedings*, page 222.

Mougiakou, E., Papadimitriou, S., and Virvou, M. (2020). Synchronous and asynchronous learning methods under the light of general data protection regulation. In *2020 11th International Conference on Information, Intelligence, Systems and Applications (IISA*, pages 1–7. IEEE.

Rajagopal, K. (2023). Personal learning environments as socio-technical systems: does decentralised data finally give us the right balance? *Revista de Educación a Distancia (RED)*, 23(71).

Rojas, M. A. T. (2020). Avaliação da adequação do instituto federal de santa catarina à lei geral de proteção de dados pessoais.

Rosso, O. (2023). A aplicação da lgpd nas universidades brasileiras. Available at: https://posts.desafiosdaeducacao.com.br/lgpd-universidades-brasileiras/.

Santos, P., Peixoto, M., and Vilela, J. (2021). Understanding the information security culture of organizations: Results of a survey. In *Proceedings of the XVII Brazilian Symposium on Information Systems*, pages 1–8.

SERPRO (2020). Educação e LGPD: impactos e desafios nas instituições de ensino.

Sá, B. (2022). LGPD na educação: como a proteção de dados pessoais impacta o futuro das escolas. Available at: https://www.jusbrasil.com.br/artigos/lgpd-na-educacao-como-a-protecao-de-dados-pessoais-impacta-o-futuro-das-escolas/1836610975.