


Privacy Orientation during Online Teaching-Learning Activities: Practices Adopted and Lessons Learned

Mônica da Silva  [Fluminense Federal University | monica_silva@id.uff.br]

José Viterbo  [Fluminense Federal University | viterbo@ic.uff.br]

Luciana Cardoso de C. Salgado  [Fluminense Federal University | luciana@ic.uff.br]

Érica Mourão  [Fluminense Federal University | ericamourao@id.uff.br]

Abstract

The COVID-19 pandemic has shifted from traditional face-to-face teaching to technology-mediated distance learning, creating significant new challenges for teachers and students. The rapid integration of new technologies into the teaching and learning process can give rise to privacy issues. This study investigates how teachers and students of undergraduate and graduate courses in Information and Communication Technology (ICT) have been educated about protecting their privacy during online course activities. An exploratory qualitative-quantitative study was conducted, and 91 participants were interviewed to determine how they were guided to protect their privacy during online course activities. The study found that 75% of teachers consider teaching about privacy in ICT courses to be “very important”. However, these teachers still lack guidance, as 66% have not communicated privacy-related rights to their students. Furthermore, 80% have yet to communicate about websites or the location of privacy information from the educational institution. Despite some positive results identified in the study, such as 93% of teachers reporting that they are recording activities and 91% of students stating that they were informed about the recording of activities, challenges still need to be addressed regarding privacy issues during online teaching and learning activities. Therefore, the study proposes some good privacy practices that can be adopted by educational institutions, teachers, and students in the context of technology-mediated education.

Keywords: *Privacy concerns, Personal data, Institutional communication, Higher education*

1 Introduction

In 2020, the COVID-19 pandemic brought about significant changes that affected the educational process on a global scale. The transition from in-person to remote learning became an urgent need, facilitated by technology and social distancing measures (Branco et al., 2020; Mourao et al., 2021; Chang, 2021). However, in this context, critical situations related to the privacy of teachers and students became more evident (de Almeida et al., 2020).

Prior to the pandemic, teachers and students were in a more isolated environment where physical walls provided a sense of protection. However, the COVID-19 pandemic has necessitated remote classes and activities, often recorded and made available in digital environments (Chang, 2021). This shift to virtual learning can create privacy concerns for participants who may be subject to monitoring or surveillance, potentially leading to privacy violations for themselves or even for third parties (Teräs et al., 2020). However, effectively managing privacy in online environments poses a challenge for many individuals and may have diverse ramifications for offline existence Vilela et al. (2015).

According to Alier et al. (2021), educational institutions have a strong interest and incentive to collect student data through systems, which can be used both internally and by third parties, primarily for electronic advertising purposes. However, during the pandemic, reports of harassment and surveillance of teachers in educational institutions have surfaced. For instance, “Teachers Report Surveillance in Remote Classes in Pandemic” describes examples of such surveillance (Santino and Pina, 2021). Moreover, collecting

images during virtual classes can result in further privacy issues, as many individuals inadvertently reveal personal information about their private lives through webcams (Rajab and Soheib, 2021).

The COVID-19 pandemic has brought about behavioral changes across all levels of education, ranging from elementary schools to graduate courses (Teräs et al., 2020). In Information and Communication Technologies (ICT) courses, new challenges and difficulties have also emerged, such as the need for technical support and the perception of the interaction between teachers and students (Mourao et al., 2021). Moreover, the shift to online activities has exposed the privacy of teachers and students to a greater extent (de Almeida et al., 2020).

In recent years, legal developments have emerged to protect the privacy of individuals, such as the General Law for the Protection of Personal Data – *Lei Geral de Proteção de Dados Pessoais* (LGPD) in Portuguese of Brazil (Brasil, 2018), and the General Data Protection Regulation (GDPR) of the European Union (Regulation, 2016). However, in addition to legal compliance, education is essential to ensure that people understand their rights and responsibilities. To comply with the LGPD, Brazilian public and private educational institutions must provide training to those involved in the teaching process, such as teachers, employees, outsourced workers and others associated with the institution (Marković et al., 2019).

According to Egelman et al. (2016), current computer science curricula in U.S. aimed at high school and undergraduate students acknowledge the importance of privacy education, but do not provide content specific. Furthermore, many

teachers wish to educate their students on privacy but often face challenges in approaching the topic and feeling qualified to do so. There are a number of existing providers that offer some classroom materials on online privacy, but privacy is one topic among many, not the primary focus of the course.

In Brazil, it is necessary to invest in means of education and communication that are more direct, simple, and aimed at a better understanding of those involved in (Information and Communication Technology (ICT) courses (Vittorazzi et al., 2019). Privacy concerns are also significant obstacles, as highlighted by the Brazilian Computer Society (SBC) in the “Great Challenges for Research in Information Systems in Brazil for the period from 2016 to 2026”, where challenges related to privacy in information systems, big data processing, smart cities, and data privacy are identified (Boscarioli et al., 2017).

Recent studies have highlighted a growing concern about student and teacher privacy during online activities in various countries, including South Korea (Kim, 2021), Spain and Norway (Gudmundsdottir et al., 2020), and the USA (Balash et al., 2021). Discussing the impact of the COVID-19 pandemic on higher education in Taiwan, a study by Peng and Dutta (2022) observed that students were not adequately prepared for online learning, leading to a reduced concern for privacy. However, our literature review did not identify any studies addressing best practices for personal data protection in online educational activities in Brazil, particularly in the field of ICT courses.

In this work we analyze the adoption of privacy protection practices in online teaching-learning activities in undergraduate and graduate ICT courses conducted during the COVID-19 pandemic in 2020 and 2021, extending the work by da Silva et al. (2022b). Specifically, we identified the following Research Question (RQ): **“How have institutions, teachers, and students of undergraduate and postgraduate courses in ICT been advised to deal with privacy issues during remote activities during the COVID-19 pandemic?”**

To answer this Research Question, we planned and conducted survey research using google forms online¹ (Fink, 2003; Sue and Ritter, 2012). We sent our survey to potential respondents in several Brazilian institutions and received 91 responses. In the analysis of the results, we identified areas in which online activities can be improved to more effectively protect the privacy of stakeholders in distance education, primarily students and teachers. As an additional contribution, we presented a set of lessons learned that can be implemented by institutions, teachers, and students to ensure privacy during online teaching and learning activities.

This work is organized as follows: section 2 presents the related works with our research. In section 3, we describe the research methodology, explaining the study design, data collection and analysis. In section 4, we present the analysis of the results, and in section 5, we discuss the results. In section 6, we present the lessons learned from the literature review and the research conducted. In section 7, we present the threats to validity. Finally, in section 8, we present the final considerations and future works.

2 Related Works

Recently, the importance of ensuring data privacy has been emphasized, and technologies that provide privacy can generate greater engagement among users of a program (da Silva et al., 2018). Therefore, it is crucial for students of ICT courses, especially those who will work on creating new technologies, to understand multidisciplinary requirements such as ethics and privacy to work effectively with privacy specialists in teams (Tahaei et al., 2021).

However, a study by Vittorazzi et al. (2019) found that 95% of students rarely or never read the privacy policy before installing a program, suggesting that even people with computer science knowledge may not prioritize protecting their data. This data is supported by a study that found that only 14% of participants, teachers, and students in ICT degree programs read privacy policies when using social networks and apps (da Silva et al., 2022a).

A literature review conducted by de Almeida et al. (2020) looked for ethical, privacy, and security issues in online or distance education in Brazil. They found that there is not yet legislation that fully covers ethics, privacy, and security in education. At the same time, there are many opportunities for related studies and information on handling personal data in these areas.

The research conducted by Prinsloo et al. (2022) emphasizes that modern technological advancements often assume that individuals have control over their personal data and voluntarily share this information while using online resources. However, when technology is integrated into educational settings, students’ privacy can be threatened by these tools. Nonetheless, privacy education entails imparting digital literacy skills to learners so that they may comprehend the workings of these systems, consequently enhancing their privacy protection. The author contends that Privacy-Enhancing Technologies (PETs) are crucial in safeguarding students’ privacy, they are not a panacea and possess inherent limitations.

With the advent of privacy legislation such as GDPR, LGPD, and CCPA, professionals at various educational levels have realized the importance of addressing privacy in the curriculum for better digital education (Soares et al., 2020). Institutions can provide materials and content where teachers and students can understand technical and social principles to protect their privacy (Egelman et al., 2016).

In the study by Egelman et al. (2016), solutions for teaching privacy were proposed for laypersons, high school and undergraduates in the United States. The author presents the Teachers’ Resource for Online Privacy Education (TROPE) and describes the Teaching Privacy Project (TPP)². Games are also used to teach privacy to different age groups (Gioia et al., 2019; Pérez et al., 2020).

The study by Freitas and da Silva (2021) aims to find out how higher education institutions in Portugal adapt online education to the GDPR. The study used a questionnaire that obtained 99 responses from students from different higher education courses. The study obtained information on privacy and security issues observed in online activities during the pandemic. This study observed that 63% of the partici-

¹<https://docs.google.com/forms/>

²Teaching Privacy Project - <http://teachingprivacy.org>

pants were not informed about the recording and audiovisual processing of their data. Another privacy issue in the study was that 46% of participants could access and maintain documents with grades from colleagues on their devices.

The study by Peng and Dutta (2022) conducted an empirical investigation exploring the impact of personality traits and information privacy concerns on adopting e-learning environments during the COVID-19 pandemic in Taiwan. The study found that openness to experience and awareness was positively associated with e-learning adoption, while neuroticism was negatively associated. Concerns about information privacy have been found to have a negative impact on e-learning adoption. The study highlights the importance of addressing information privacy issues in promoting the adoption of e-learning environments.

We reviewed two studies on teaching privacy and security in computer science courses. One of the studies, conducted by Cristani et al. (2020), evaluated the state of information security education in Brazilian computer science courses using both curriculum information and a questionnaire. The study revealed a pressing need to improve students' comprehension of security and privacy topics and identified the necessity for further research in the field. Dragoni et al. (2021) investigated the extent to which European universities prepare students to build secure systems. The study revealed that many programs need to emphasize security and privacy in their curricula, and differences were found between the curricula of ICT courses in different countries. These studies provide insights into the current state of privacy and security education in computer science courses and highlight the need to improve the curricula to address these issues adequately.

Based on the papers above that focus on ethics, privacy policy, and security, our study is broader and more up-to-date, covering the papers published in the last five years. In terms of goals, our study has the most comprehensive focus, since: (i) it does not focus on respondents of a specific discipline like Vittorazzi et al. (2019), who focus on respondents of three disciplines: Cryptography and Data Security, Fundamentals of Computing, or Supervised Internship; and like Prinsloo et al. (2022), who focus on student data privacy in learning analytics from a critical data studies perspective; (ii) it does not discuss in the context only of distance education like de Almeida et al. (2020), who focus on aspects of ethics, security, and privacy in the context of access, manipulation, treatment, and availability of teacher and student data provided by Virtual Learning Environments; (iii) it does not discuss in the context of the U.S. like Egelman et al. (2016), who focus on solutions for teaching privacy alignment with U.S. curriculum standards.

Finally, our study is unprecedented, and the main advancement of our work is that it analyzes the adoption of privacy protection practices in online teaching-learning activities in undergraduate and graduate ICT courses conducted during the COVID-19 pandemic in 2020 and 2021 in Brazil. It provides a set of lessons learned that can be implemented by institutions, teachers, and students to ensure privacy during online teaching and learning activities.

3 Method

This is an exploratory and descriptive research that involved a bibliographic survey and qualitative-quantitative research carried out through an online form on Google Forms³ (Gil, 2002; Wohlin et al., 2012). The survey was distributed to teachers and students of ICT courses in Brazil, with no selection of private courses, institutions, or Information Technology (IT) disciplines.

For the design, implementation, and interpretation of the results of the data collected during the study, we employed the *Objective/Question/Metric* (GQM) paradigm (Basili and Rombach, 1988). The GQM paradigm is an approach to defining and evaluating operational goals using measurements. It represents a systematic approach in which objectives are defined operationally, refined into quantifiable questions to extract appropriate information (Basili, 1993).

3.1 Study Design

According to GQM paradigm (Basili and Rombach, 1988), our study aims to *analyze* privacy-related issues and identify the practices adopted and lessons learned *for the purpose of* evaluation *with respect to* privacy guidelines presented *from the point of view of* teachers and students by educational institutions, as well as the guidelines that teachers pass on to students *in the context of* online teaching and learning activities carried out in undergraduate and graduate ICT courses in the years 2020 and 2021.

Following the GQM approach, we designed a set of questions addressed to all participants to assess their general knowledge and opinions on the subject, as presented in Table 1. These questions were rated on a 5-point Likert scale (1 – Never; 2 – Rarely; 3 – Occasionally; 4 – Often; 5 – Always). It is worth noting that the Likert scale, as mentioned by Harpe (2015), is no longer strictly used solely for measuring interviewee agreement but can be employed for evaluating frequency, importance, and other relevant factors.

After gathering participant characteristics, we asked them to specify whether they had assumed the role of teachers or students in the years 2020 and/or 2021.

Participants who identified themselves as teachers answered specific questions presented in Table 2. One of the questions was of the multiple-choice type, and the others were of the 5-point Likert type. We defined for each one the maximum value (“Ever”), the minimum value (“Never”), and the middle value (“Occasionally”). At the end of the questionnaire aimed at teachers, we included an open question to collect information about privacy challenges related to the teaching process in ICT courses.

Participants who identified themselves as students answered specific questions presented in Table 3. Some questions were of the multiple-choice type, with the possibility of including a free text option for students to provide additional answers. At the end of the questionnaire directed at students, we added an open question to collect information about the privacy challenges that the students identified.

To structure most of the questions in this study, we used the studies of Freitas and da Silva (2021); de Almeida et al.

³<https://www.google.com/intl/pt-BR/forms/about/>

(2020), which also focused on privacy observations in teaching across various courses. The participant profile data is presented in section 4.1 as the last section of this paper.

3.2 Data Collection

To perform data collection, the Google form was available from January 27th, 2022 to February 28th, 2022. This form was structured with four sections: (1) participant characterization, which included questions about the participant's profile; (2) questions directed to students of ICT courses; (3) questions directed to teachers of the ICT courses; and (4) questions addressed to all participants. The survey focused on teaching and learning activities during the years 2020 and 2021, given the implementation of LGPD 2020 and the COVID-19 pandemic.

The target audience was reached through emails and WhatsApp groups composed of undergraduate and graduate students and teachers in ICT. As the researchers conducting the study are affiliated with UFF, social media and emails from UFF's undergraduate and graduate ICT courses were used to distribute the survey. Additionally, other researchers known to the authors and working with undergraduate and graduate ICT courses were contacted to respond to and share the survey. Participants were also asked to forward the survey to other potential participants who belong to the group of interest. However, this process created a bias in the study as there was a higher participation rate from UFF members

3.3 Ethical Criteria and Procedures Adopted

In this subsection, we deliberate on the ethical criteria and procedures employed during the execution of the research which forms the backbone of this article. It is imperative to state that in Brazil, research involving humans is dictated by specific guidelines, such as Resolution No. 466/2012 (Brasil, 2013) and Resolution No. 510/2016 (Brasil, 2016), both promulgated by the National Health Council (of Portuguese Conselho Nacional de Saúde (CNS)).

Resolution No. 466/2012 mandates that "research projects involving human beings must conform to the stipulations of this Resolution," accentuating that "research involving humans must uphold appropriate ethical and scientific principles." Thus, adherence to these guidelines is indispensable for the validity and ethical integrity of the research project.

In the scope of Resolution No. 510/2016, which regulates non-invasive studies involving human subjects, we adhered to its guidelines in our analysis of the research conducted via an online form, incorporating the Informed Consent Form (ICF), also known as Termo de Consentimento Livre e Esclarecido (TCLE) in Brazil, issued by the Ethics Committee (CEP) of UFF⁴. Regrettably, there was insufficient time to submit the project to the Ethics Committee, yet we adhered to the terms of informed consent in our studies as provided by the CEP.

Subsequently, we underscore the ethical criteria and procedures we employed in our study to comply with the recommendations embodied in Resolution No. 510/2016, primarily in its Article 17.

1. It is imperative to obtain the informed and voluntary consent of the research participant. In soliciting participation, we dispatched a message detailing the researchers accountable for the study, the methods of contacting them, and the institution they are associated with. The objective of the study, which is to evaluate specific guidelines, was also illuminated. Accompanied by the invitation, we dispatched the ICF, wherein participants are accorded a succinct explanation of the study's objectives.
2. "Justification, objectives, and procedures to be utilized in the research, accompanied by information regarding the methods to be implemented": The study which instigated this research was executed during a period when online data collection proved more viable due to restrictions on direct contact imposed by the COVID-19 pandemic. The pandemic also served as an impetus for conducting this research. The objective of the study - to evaluate specific guidelines - was reiterated. Alongside the invitation, we forwarded the ICF, where participants were given a brief explanation about the study's objectives. In our study, participants had access to information regarding the data that would be collected and the procedures for collection via the ICF.
3. "Explicitation of potential harm resulting from participation in the research": The form was made accessible online, allowing the participant to opt for the most convenient time and location to complete it. Additionally, the participant had the choice to interrupt and resume filling out the form at a different time, without loss of previously entered information. The data collected were impersonal and were anonymized prior to usage. To alleviate fatigue, the form was structured in sections. All participants filled out demographic data, but upon identifying as students or teachers, they answered specific questionnaires. The form was designed to store partial responses, enabling participants to complete the form at different times, at their convenience.
4. "Guarantee of the participant's total freedom to decide on their participation in the research": Participants were informed, via the ICF, that they could withdraw from the research at any moment, without any detriment.
5. "Assurance of maintaining the confidentiality and privacy of the participants": The third paragraph of the ICF elucidates that all collected data is intended for scientific research in the field of education and that all data will be anonymized to prevent the identification of participants. The data was held confidential, stored in an institutional account accessible only to the researchers. The information shared in scientific articles was anonymized.
6. "Assurance to participants of access to research results": Participants could request the research results and/or scientific publications resulting from the study at any time via email or telephone.
7. "Explicitation of the guarantee to the participant of reimbursement": Participation in the study should be voluntary, without any financial compensation. Participants were invited, via online (email and social networks), to partake in the research voluntarily and optionally.

⁴Ethics Committee (CEP) - <http://cep.uff.br/>

Table 1. Questions and metrics addressed to teachers and students.

ID	Question	Type	Metrics (possible answer)
Question 01	How important do you think teaching privacy/personal data protection is for the ICT course curriculum?	Likert	1 - Unimportant, 2 - Little important, 3 - Reasonably, 4 - Important, 5 - Very important
In 2020 and/or 2021, how often did you study or seek information on the topics. For questions 02 to 05:			
Question 02	What is personal data?	Likert	Never; Rarely; Occasionally; Frequently; Ever
Question 03	How to control (edit, update, remove) data collected in App?	Likert	Never; Rarely; Occasionally; Frequently; Ever
Question 04	General Personal Data Protection Law (LGPD)?	Likert	Never; Rarely; Occasionally; Frequently; Ever
Question 05	General Data Protection Regulation (GDPR)?	Likert	Never; Rarely; Occasionally; Frequently; Ever

Table 2. Questions and metrics addressed to teachers.

ID	Question	Type	Metrics (possible answer)
Question 06	In 2020 and/or 2021, have you received any guidance /manual/documentation, from the educational INSTITUTION that addresses privacy issues when using videoconferencing platforms?	Multiple choice	a) I NEVER received any guidance from the institution regarding LGPD or privacy. b) How to inform the student of the rights in relation to the LGPD. c) How to proceed in activities that were being recorded. d) How requested consent for the use of personal data. e) How to guide students to avoid showing up during recording. f) How to organize, store and delete recorded videos. g) How long videos could be stored/used. h) How to inform the beginning of the recording in the class/activity. i) How to properly communicate grades to students. j) What were the educational institution's rules on personal data protection. k) Communicated who the DPO (data protector) is at the educational institution.
In online teaching activities in 2020 and/or 2021, identify how often you carried out the guidelines below. For questions 07 to 14:			
Question 07	Communicate to students their rights under the LGPD	Likert	Never; Rarely; Occasionally; Frequently; Ever
Question 08	Inform that the activity was being recorded	Likert	Never; Rarely; Occasionally; Frequently; Ever
Question 09	Request authorization for recording	Likert	Never; Rarely; Occasionally; Frequently; Ever
Question 10	Guide the student on how to avoid appearing during recording	Likert	Never; Rarely; Occasionally; Frequently; Ever
Question 11	Inform where the videos would be being used	Likert	Never; Rarely; Occasionally; Frequently; Ever
Question 12	Inform what was the purpose of recording the activity	Likert	Never; Rarely; Occasionally; Frequently; Ever
Question 13	Inform how long the videos would be stored/used	Likert	Never; Rarely; Occasionally; Frequently; Ever
Question 14	Inform a website/link where the institution's privacy policy were	Likert	Never; Rarely; Occasionally; Frequently; Ever
Question 15	For you, what are the challenges faced in the teaching process about privacy in ICT courses?	Open question	

8. "Information about the address, email, and telephone contact of the research's responsible party": The data of the researchers, email, telephone, the institution they are affiliated with, and the name of the research project were included in the ICF.
9. "Information that the participant will have access to the consent record whenever requested": The responsible researcher's email and telephone were provided, enabling participants to request the form at any time.

3.4 Data Analysis

To ensure the reliability of the survey results, we adopted several measures during the analysis phase: (i) we anonymized the data, (ii) we cleaned the data to remove incomplete responses, (iii) we assigned a unique identifier to each participant's responses, and (iv) we ensured that the sum of the percentages on the five-point Likert Scale equals one hundred percent during the results discussion.

Regarding the open-ended questions, we analyzed the responses and presented the participants' direct mentions in the context of the challenge question. These responses were used

Table 3. Questions and metrics addressed to students.

ID	Question	Type	Metrics (possible answer)
Question 16	In 2020 and/or 2021, have you received any guidance /manual/documentation, from the an educational institution or teachers, that addresses privacy issues when using videoconferencing platforms?	Single option	Yes; No
Before or while carrying out online activities in 2020 and/or 2021, how often did you receive the following guidelines. For questions 17 to 24:			
Question 17	I was communicated about my rights under the LGPD	Likert	Never; Rarely; Occasionally; Frequently; Ever
Question 18	I was informed that the activity was being recorded	Likert	Never; Rarely; Occasionally; Frequently; Ever
Question 19	I was asked for permission to record	Likert	Never; Rarely; Occasionally; Frequently; Ever
Question 20	I received guidance on how to avoid appearing while recording	Likert	Never; Rarely; Occasionally; Frequently; Ever
Question 21	It was informed where the videos will be used	Likert	Never; Rarely; Occasionally; Frequently; Ever
Question 22	The purpose of recording the activity was informed	Likert	Never; Rarely; Occasionally; Frequently; Ever
Question 23	It was informed how long the videos would be stored/used.	Likert	Never; Rarely; Occasionally; Frequently; Ever
Question 24	A website/link containing the institution's privacy policies are informed	Likert	Never; Rarely; Occasionally; Frequently; Ever
Question 25	Regarding the dissemination of results/exam scores /works carried out in 2020 and/or 2021, choose the option that you witnessed the most:	Single option or open question.	a) The activities I performed did not have grades b) The results/scores only appeared for you or you received an individual news (email, WhatsApp, etc.) c) I needed to access a system with a username and password. c) He could see his results and those of colleagues. d) Others
Question 26	When you had access to classmates' grades, which of the following situations occurred:	Multiple choice or open question.	a) I was able to download the file with all the grades to my device. b) I could see it for a while. c) I have had access to the grades for a long period of time (+ 6 months) or I still have. d) I could see classmates' grades, however, only the registration number and grade appeared. e) Others
Question 27	What challenges do you, as an ICT student, face about the privacy theme?	Open question	

to support the discussions presented in this paper.

It is important to note that we did not perform any statistical analysis of the closed single or multiple-choice questions, as well as the open-ended questions. This is because such an analysis is beyond the scope of this phase of the study.

4 Results

This study was responded by ninety-five (95) participants. However, four (04) responses were not included because they needed to be completed. Of a total 91 (ninety-one) accepted responses, 76 (83.52%) participants answered the student questions, 13 (14.29%) answered the teachers questions, and 02 (2.20%) responded in both profiles. The dataset of this work is available in Zenodo and can be accessed via the link: <https://doi.org/10.5281/zenodo.7853572>.

4.1 Respondents' demographics

Out of the 91 respondents who completed the questionnaire, 13 identified themselves as teachers, 78 as students, and 2 as both teachers and students. The main data are described

below and presented in Figure 1. We found that 49% of the participants were between 18 and 29 years old, 21% were between 30 and 39, 20% were between 40 and 49, 7% were between 50 and 59, and 3% were over 60.

Regarding the educational levels of the 78 participants who identified themselves as students, we found that they were distributed as follows: 62.82% were undergraduates, 23.08% were master's students, 12.82% were doctoral students, and 1.28% were postdoctoral students.

Gender representation showed that 26% of the participants were female, 73% were male, and 1% preferred not to specify. Affiliation with private institutions was reported by only 2.20% of the participants, while 97.80% indicated a connection to public institutions. As such, this study is more focused on public universities.

Regarding location, 74.3% of the participants were from Rio de Janeiro, followed by 12.6% from the state of Mato Grosso, 4.2% from Acre, and 3.2% from the Federal District. Most of the students were from the Fluminense Federal University (UFF), representing 78.2% of the participants, followed by the Federal University of Mato Grosso (UFMT) with 7.3%, the Federal Institute of Mato Grosso (IFMT) with

4.2%, and the Federal University of Acre (UFAC) with 4.2%. The research was conducted by students from the Institute of Computing at UFF, which may have influenced the perspective of teachers and students from the Computing Undergraduate and Postgraduate courses at UFF.

4.2 Analysis of questions addressed to teachers and students

This section presents the findings of a survey conducted with 91 participants to investigate their knowledge and perception of privacy and legislation, including the Brazilian General Data Protection Law (LGPD) and the European General Data Protection Regulation (GDPR). To determine whether the participants considered teaching privacy to be relevant and necessary, we formulated the following question: **Question 01) How important do you think teaching privacy/protection of personal data is for the curriculum of ICT courses?** Participants were asked to rate the importance on a scale of 1 (unimportant) to 5 (very important).

The results of Question 01 are presented in Figure 2, which shows that 75% of participants considered the inclusion of privacy in ICT courses to be very important. For 19% of the participants, it was important to include the topic in courses, and for 5%, it was considered reasonably necessary. When we analyzed the same question separately for teachers and students, we found that the results were very similar, with no significant discrepancies between the two profiles.

To assess the participants' knowledge levels and research habits on the topics covered in the study, we formulated questions 02 to 05 based on Table 1. Figure 3 presents the answers, with percentages (%) on the left representing the union of the "never" and "rarely" responses, percentages on the right representing the union of the "frequently" and "ever" responses, and the intermediate results showing "occasionally" responses.

The responses to **questions 02 to 05** indicate the need for students to be more proactive in seeking information on privacy-related issues. When we asked participants if they know what personal data is (question 02), we found that 26.4% never searched for information, 20.9% rarely did, while 27.5% occasionally sought information, and a total of 25.3% frequently or ever searched for information.

In question 03, we found that 29.7% of participants ever or frequently seek information on how to edit, remove, or update their data, that is, being able to control their data. While another 33% do so occasionally. However, 37.3% of participants never or rarely searched for this information.

To evaluate participants' awareness of legislation related to privacy, we formulated question 04 regarding the LGPD and question 05 regarding the GDPR. For question 04, 41.8% of participants reported that they never or rarely search for information related to the LGPD, while 37.4% occasionally search for information and 20.9% ever or frequently search for information. This is a relatively positive result, especially considering that the survey was conducted in Brazil. However, when it comes to the GDPR, European legislation mentioned in question 05, we found that only 15% of respondents ever or frequently seek information, while 31.9% occasionally do so and 52.8% never or rarely do. This suggests a lower

awareness of GDPR compared to LGPD among the participants.

4.3 What privacy orientations did teachers receive and carry out?

This section presents the responses of 15 teachers to **Questions 06 to 15**, which aimed to identify whether and how educational institutions provided guidance to teachers on privacy during online teaching activities amidst the COVID-19 pandemic.

Question 06 aimed to identify the guidelines, such as manuals, guides, and documents, provided by the institution to teachers regarding the use of video conferencing platforms for teaching activities. This question offered multiple choice answers, and participants were given the option to add their own if none of the provided options were suitable. From the results, it was found that 40% of the teachers had not received any guidance from the institution regarding privacy issues associated with the use of video conferencing in teaching activities (letter "a" of question 6).

Conversely, 60% of the participants had received guidance, which varied between options "b to k" in question 06. Of those who received guidance, 40% had received guidance on how to handle activities that were being recorded. Additionally, 26.7% had received guidance on how to obtain consent for the use of personal data, while 20% had received guidance on how to instruct students not to appear in recordings. 13% of the teachers reported receiving guidance on the storage and organization of videos, including the length of time videos can be stored, and how to delete them. 20% of teachers had received guidance on informing students of their rights under the LGPD. 6.7% of the teachers had received guidance on presenting grades to students. The same percentage of participants had received guidance from the institution's Data Protection Officer (DPO) or Data Protector, and the institution's data protection standards. One teacher reported receiving LGPD guidance from the institution, but noted that it was not related to teaching processes.

Regarding the orientations that the teachers carried out involving situations that impact students' privacy, the answers to questions present in Table 2 can be observed in Figure 4. Based on the data obtained, it is possible to observe that the results on the left are those with negative points, and those on the right are the ones with positive points.

A negative point to note in question 14 is that 80% of teachers never and 7% rarely informed about the institution's privacy policies. This may have occurred because the teachers were unaware of the information. This result is directly related to question 07, where 73.3% of teachers reported that they are never or rarely aware of their rights related to LGPD for students. In question 13, 53.3% of teachers never informed students about the time of storage and use of videos, and 7% rarely provided guidance. In question 10, 40% of teachers never guided students on ways to avoid appearing in recordings, and 7% rarely did.

On the other hand, some positive points were observed, as seen in Figure 4. For instance, in question 08, 93% of the teachers reported when the activity was being recorded. For question 12, 60% ever and 20% of the participants frequently

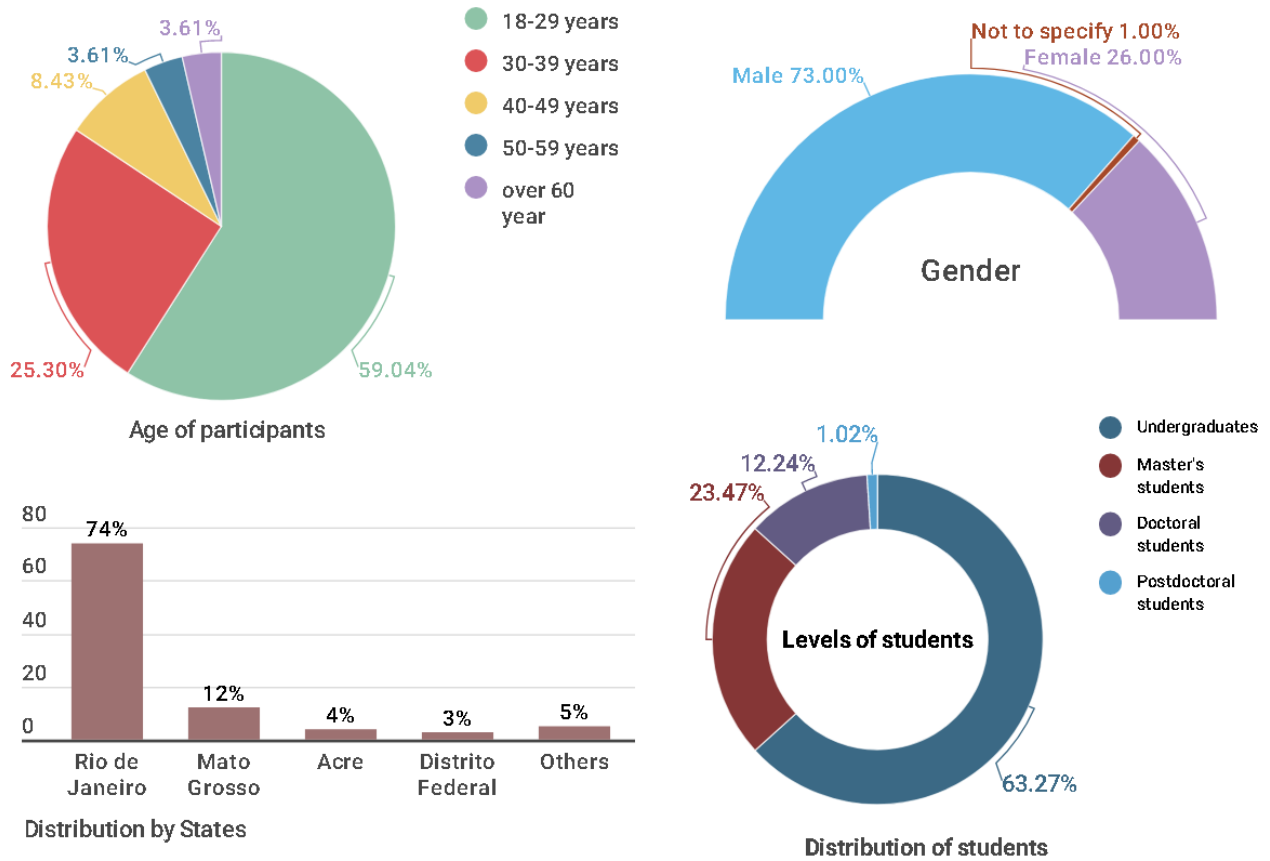


Figure 1. Participants profile infographic

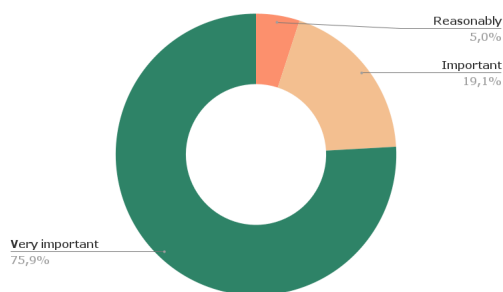


Figure 2. The results of question 01.

informed the purpose of recording the activity. In question 09, 46.6% ever and 26.7% frequently asked students for permission to record. In question 11, 53.3% of teachers informed students where the video was being used or for what purpose. This information is consistent with that reported by students, as shown in Figure 5.

Among the 15 professors analyzed, 46.67% were **affiliated with UFF**, while 53.33% were associated with **other higher education institutions** in Brazil. To assess whether there were differences in information between the two groups of teachers, we conducted separate analyses of the data presented in the paragraphs below.

Comparing data from UFF professors with those from other institutions, differences were observed in some questions answered. In question 07, 86% of UFF professors reported that they had never communicated LGPD data to their students. Conversely, the proportion of professors who had never conducted orientations decreased to 50% among

those from other institutions, indicating that some institutions are more advanced in the process of communicating about LGPD.

Regarding question 08, which inquired whether teachers informed their students that they were being recorded, we found that 86% of UFF faculty always provided such information, while among teachers from other institutions, the proportion was 100%. The values between UFF teachers and those from other institutions did not show much difference when positive responses (ever and frequently) were combined for question 09, which asked whether teachers obtained authorization from students to record.

In question 10, which assessed the frequency with which teachers instructed students not to appear in recordings, we observed that 57% of UFF teachers had never provided such guidance. This value decreased to 25% among teachers from other institutions who had never provided such instruction, while 12% had rarely done so, and 50% ever or frequently provided such instruction.

Regarding the guidance provided to students on the purpose of recording classes (question 11), we found that 72% of teachers ever or frequently provided such information, while among teachers from other institutions, the proportion was 62%. Concerning the description of the purposes of recording classes (question 12), the proportion was constant among UFF teachers, with 72% of them ever or frequently providing such guidance. However, for the same question, 87% of teachers from other institutions reported ever or frequently providing such guidance.

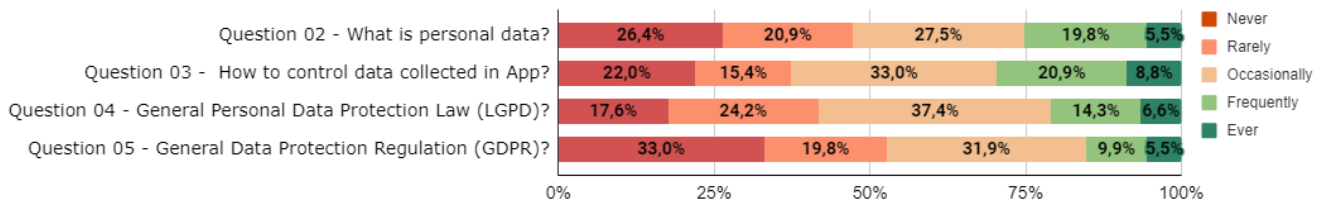


Figure 3. Overview of all participants on topics related to privacy.

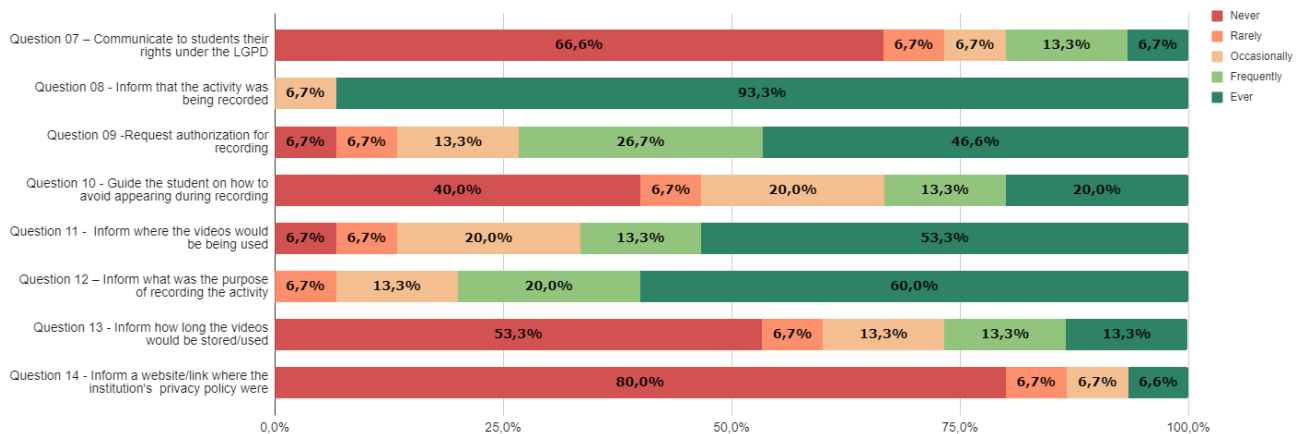


Figure 4. Guidance on privacy provided by teachers in online teaching activities.

When asked about informing students of the length of time that recordings would be stored (question 13), a significant difference was observed, where 86% of UFF teachers reported never providing such communication. In comparison, this value decreased to 25% among teachers from other institutions.

Finally, about question 14, which investigated whether teachers had guided their students on the location of their institution's privacy policies, we found that 86% of teachers had "never" provided such communication, while this proportion was 75% among teachers from other institutions.

To gain insight into the challenges faced by ICT teachers regarding privacy during their activities, we asked the following **Question 15) For you, what are the challenges faced in the teaching process about privacy in ICT courses?** The responses revealed the complexity of the topic, with one participant noting that "A challenge is for the Educational Institution to publicize more about the topic and clarify the importance of privacy so that this information reaches everyone."

Another participant commented on the difficulties of approaching the topic in a broader teaching environment beyond online activities, stating that "as it is a new topic, not even the teachers (or managers) have the confidence to talk about it. I think I would still need training or something." This point was echoed by another teacher who said, "About personal privacy, related to remote classes, I believe we require more guidance from the University."

The teachers highlighted the need for more training and information to improve their understanding of privacy issues, which results in a lack of information when carrying out their activities. One participant pointed out that "Indicating rules according to legislation" is a challenge. These training and improvements must be constant and should involve not only the institution but also teachers, employees, and students to promote ethical use of ICT (de Almeida et al., 2020).

One participant highlighted the comprehensive nature of the issue, stating that "regarding the subjects' privacy and contents covered, I believe that the greatest challenge is knowing how to include the subject in the contents currently given, especially in subjects where human vulnerabilities are not exploited. A typical example of a discipline I could address and do not know if it does is the database discipline. We cannot leave to deal with the laws in the data delivery, that is, in the interface. The treatment must be from the collection and storage." Another participant emphasized the need for multidisciplinary discussions, stating that "I believe that the greatest challenge is to have a multi- or transdisciplinary discussion, that is, all courses must discuss these issues, regarding their specific topic, in addition to have a more complex view of how the other courses are dealing with the topic."

Research opportunities include finding ways to provide simple and applicable guidance for teachers and students to carry out their teaching/learning activities while encouraging them to think about privacy not only during remote activities but also during the process of creating or producing new technologies da Silva et al. (2023).

4.4 What privacy guidance did students receive?

This section presents the findings from a survey conducted with a total of 78 students. The questionnaire was designed to investigate the process of guidance and presentation of privacy information, how grades were presented, and whether students had access to private information of their peers, such as names and grades. However, the sudden shift from face-to-face education to remote education without adequate preparation can lead to privacy issues (de Almeida et al., 2020).

In **Question 16**, the respondents were asked whether they received any guidance or documentation from their educa-

tional institution or teachers in 2020 and/or 2021 that addressed privacy issues when using videoconferencing platforms. The results revealed that 61.5% of the students had not received any guidance, while 38.5% had.

Questions 17 to 27 were formulated to identify the respondents' answers to the statement, **Before the beginning of the recordings of the classes or in the performing online activities, how often did you receive the instructions below.** First, we present the results of **Questions 17 to 25.**

The results depicted in Figure 5 raised some concerns, such as in question 17, where 53.8% and 19.2% of the participants never or rarely, respectively, received guidance on their rights related to GDPR. Question 20 showed that 41% of the students had never received guidance on how to avoid appearing on recordings. Furthermore, 66.7% of the students were never informed about how long the video would be stored (question 23), while 62.8% and 17.9% of the participants never or rarely received any guidance on where to locate the institution's privacy policies (question 24).

However, some positive points could be observed in Figure 5, where some orientations were already being carried out, such as in question 18, where 70.5% of the participants were always informed, and 20.5% were frequently informed that the class was being recorded. The results of this study are comparatively better than a similar study conducted by Freitas and da Silva (2021), in which 51% of the students recalled receiving information about recording activities, while 32% did not remember receiving any guidance.

The results presented in Figure 5 are encouraging, with 39.7% of students ever and 28.2% frequently requesting authorization to record activities in question 19. In question 21, 39.5% and 28.2% of participants ever or frequently, respectively, were informed about the storage location of class videos. Additionally, in question 22, 51.3% of students and 19.2% were frequently aware of the purpose of the recording. These findings suggest that institutions are taking appropriate steps to ensure that students are aware of security and privacy risks related to videoconferencing programs.

After presenting the general results of questions 17 to 24 in Figure 5 and the preceding text, we analyzed responses from students at UFF and those from other institutions separately. This was necessary because 78.2% of the participants in this study were from UFF. To better understand whether there were differences in the information and guidance received by the students, we structured the data analysis graphs separately for UFF students and students from other institutions.

Figure 6 shows the results of the responses from UFF students, while Figure 7 shows the results of the responses from the remaining 21.8% of the research participants.

Some differences can be observed in the answers provided by the participants. For instance, in question 17, we observed that 69% of UFF students had yet to receive any communication about the General Data Protection Law (LGPD). This number was even higher among students from other institutions, where 82.3% of participants still needed to receive information about the LGPD.

As for question 18, there was a significant difference, with only 3.6% of UFF students reporting that they never or rarely received guidance on recording activities. However, this result jumped to 23.6% among students from other institutions,

who reported never or rarely being informed that they were being recorded. However, this value difference was not noticeable in question 19, which assessed whether authorization was requested for recording, as the results for UFF students and students from other institutions were similar.

A difference was observed in assessing whether students were advised on how to avoid recording (question 20), with 58.8% of students from other institutions saying they had never received this guidance. In contrast, this value was lower among UFF students, with 34.5% reporting never receiving guidance.

In question 21, which assessed whether guidance was provided on what the video of the class would be used for, only 23.6% of UFF students stated that they never or rarely received guidance, whereas this value was higher for students from other institutions, totaling 35.2%. Similarly, this difference was also noticeable in question 22, where 29.4% of students from other institutions stated that they had never or rarely been informed about the purpose of recording the class. At the same time, this value was much lower among UFF students, corresponding to 12.7%.

When we asked students whether they had received guidance on how long the video would be stored for use (question 23), we observed a large difference between UFF students, with 74.5% stating that they had never received guidance. However, among students from other universities, 52.9% said they had never received guidance, while 23.5% reported that they rarely received guidance.

Another difference in results between students occurred in question 24, which assessed whether they had received guidance on the link or website where the institution's privacy policies were located. In this question, only 1.8% of UFF students declared having received guidance, whereas 29.4% of students from other institutions declared receiving guidance ever or frequently.

Participants could include more information in addition to the objective questions from 17 to 24. Information from other guidance received complemented the questions above. Among these complements, we highlight *"the availability of a link to watch classes without recording them"*. Another participant highlighted that he received guidance that *"it is not allowed to disclose the videos of the classes outside the classroom (online) and to outsiders (people)"*. Students were also advised *"the material would be shared via a link via email to students (in the case of courses)"*. These contributions helped identify good practices being applied in institutions, which can be observed during the student orientation process.

In question 25, we asked participants about the dissemination of results/scores of tests/works carried out in 2020 and/or 2021. Results show that 28% of students viewed grades through a login and password-protected system, while 35% received grades individually through email or other means. The study's results differ from Freitas and da Silva (2021), where 87% of students claimed to view grades individually with a login and password.

Viewing colleagues' grades becomes more complex when we consider that 26% of participants claim to have full access to colleagues' names and grades. Another 5% of participants did not perform activities with grades, while 6% reported that the grading structures were "hybrid", with some teachers pro-

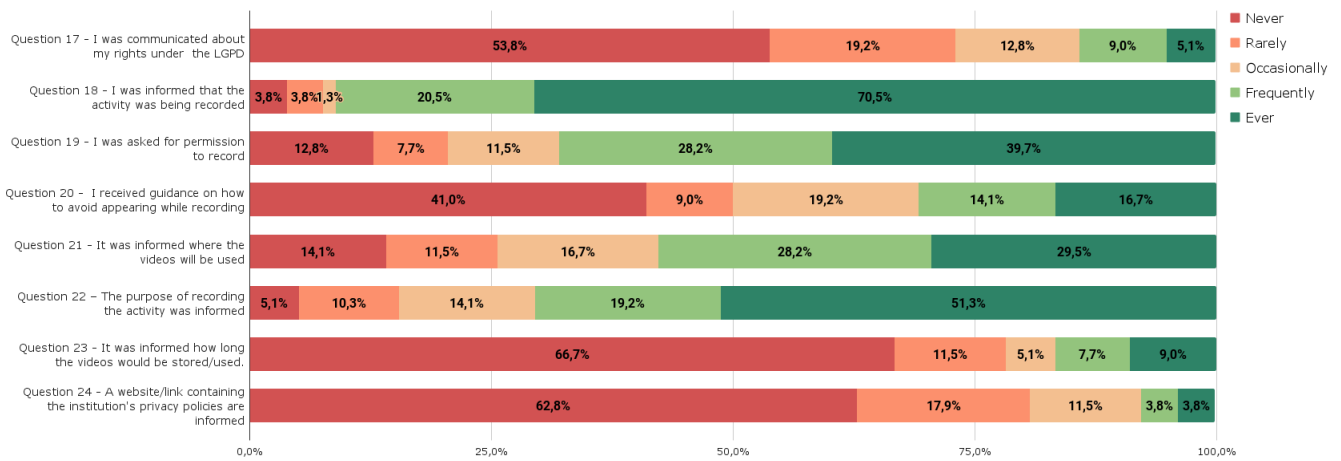


Figure 5. Guidance received by all students during online activities.

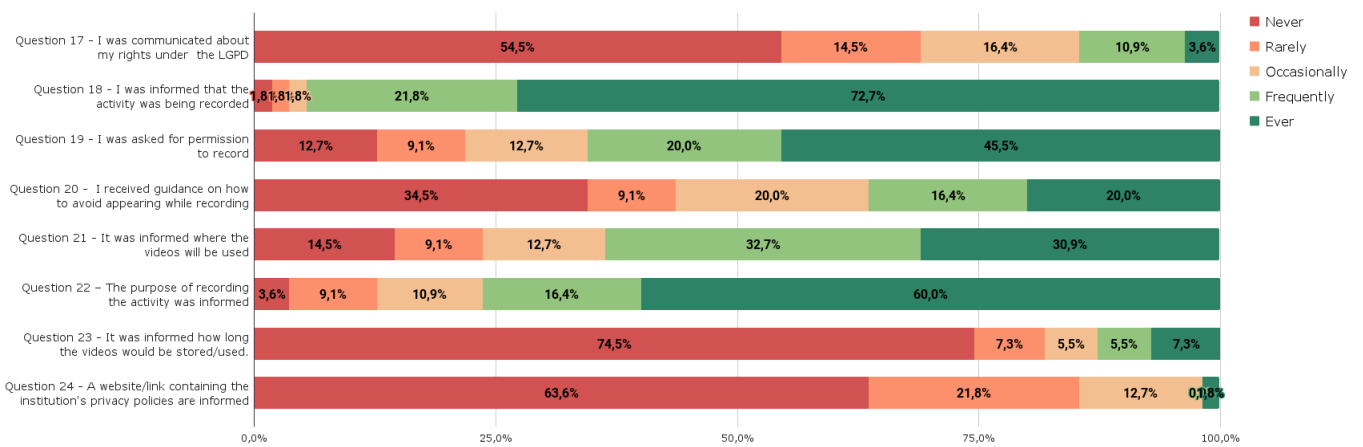


Figure 6. Guidance received by UFF students during online activities

viding grades collectively and others individually.

Question 26 was formulated to determine whether the students had access to third-party personal data, such as the grades and names of their colleagues. The question was: **Question 26) When you accessed your classmates' grades, which of the following situations occurred?** Based on this question, we observed that 59% of students were able to download all their peers' grades with their names. In their responses, 51% of the participants stated that they had seen their colleagues' grades at some point, but they did not have their names. However, other forms of identification were accessible, such as the registration number. Nonetheless, 3% reported seeing their colleagues' grades along with the initials of their names. As noted by Freitas and da Silva (2021), students should only have access to their grades. However, the author himself points out that when obtaining data from colleagues, students may end up having access to other personal information, such as courses, institution, online schedules, etc.

In terms of the duration of time that grades were visible to students, 42% of the students could access their colleagues' grades for an extended period, which exceeded 06 months or still ongoing. On the other hand, 16.8% stated that they had access to their colleagues' grades for a shorter duration, up to 6 months, while 5% had access to grades with their colleagues' names in only some subjects, without specifying

the time.

To better understand the students' perspective on privacy, an open-ended question was asked: **Question 27) What are the challenges that you, as an ICT student, face in relation to privacy?** Among the responses, privacy situations focused on behavior and emotions were observed, where one of the participants described: *"teachers do not realize that it can be a problem for some students to turn on the camera and microphone, which is a challenge for their participation in classes. They are teachers; they are not shy about showing up, and they do not know how hard it can be for some!"*

When it comes to displaying personal information such as grades, some students have expressed concerns about the potential embarrassment of displaying grades and averages of all students. One participant commented, *"The issue of grades being made public is a serious matter. The unnecessary embarrassment that some friends went through was unnecessary"*. Another participant added, *"It is not comfortable to have my grades displayed with those of my colleagues, but I understand the difficulty that the online system presents, and that it is often impracticable for the teacher to send the grades individually to each student"*.

In addition, some students have called for more information and guidance in certain courses. One participant pointed out *"a lack of clear information about what will be done with the collected data. Lack of information on the subject in gen-*

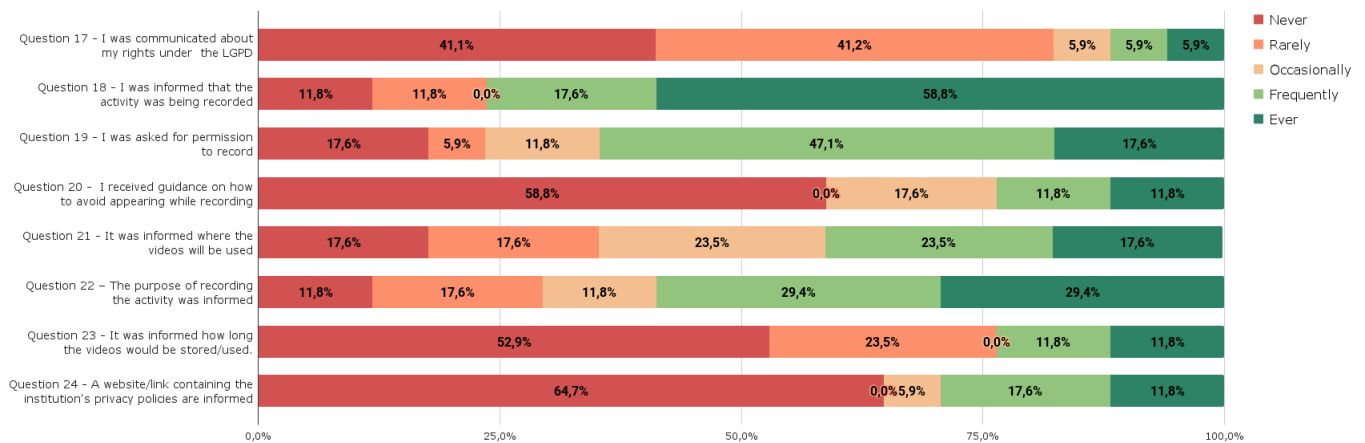


Figure 7. Guidance non-UFF students received during online activities.

eral, I don't see much discussion despite having gained space, I see that a lot is still not well clarified, or defined." However, some institutions are already protecting themselves from privacy issues in online teaching by recording classes, as the participant highlights: "in remote teaching at UFAC, teachers ask students to sign a consent form for recording the classes", this is not a complete orientation procedure, but it demonstrates how there is already a beginning of observation to the fact.

A student made an important point regarding recording activities: "I believe that due to the pandemic, the basic terms were explained when there is a recording. But when it wasn't recorded (in theory, after all, someone can record a computer screen, for example), there wasn't the same disclosure/concern." This student-provided information has been included as a practical guide to adopt, along with other observations of challenges described by students.

In terms of directly addressing privacy in teaching, many students have reported a lack of discussion and a simplistic approach. Some students feel that there is a lack of specific information and training on privacy and ethics in computing and believe this should be included in the mandatory curriculum. Privacy is reportedly only superficially covered in some elective subjects. One participant commented, "I am a graduate of the Computer Science program at UFF, and I can confidently say that I learned nothing about the LGPD during my time at university. Moreover, privacy, as a topic, was briefly mentioned by one or two professors. In summary, it is treated as a specialization subject and is not part of the undergraduate curriculum. Privacy was not even present in the information security syllabus (optional course discipline)."

Another participant also pointed to the lack of courses dealing with privacy, saying, "I have not had, until now, any specific training on privacy, and I was surprised that there is no mandatory discipline on ethics in computing. Most other courses have at least one discipline of ethics in the profession, but in computing, this ethics is a topic of discussion even by other professionals, no". Even in security-related courses, privacy is not fully covered, as described by one participant: "this topic is not covered in the classroom. Even in SecInfo classes, the focus is on algorithms and technical-mathematical procedures".

One observation is related to the execution of future activities (e.g., software development, research, uses of systems) that may require related knowledge. This participant highlights: "The main challenge as a student is to understand how to contribute to privacy after my graduation when I am already in the job market. In this way, I believe that the debate and discussion in the academy on the subject of privacy are important for the training of IT professionals".

Another challenge observed concerns understanding terms that are not common in ICT courses "understanding some legal terms", as one of the participants exemplifies. In another context, one participant points out the lack of "knowing what the best practices to be in research and data collection".

5 Discussions

The results indicate that addressing privacy in the classroom requires significant effort from all those involved in ICT courses. According to the study by Soares et al. (2020), investing in digital education, particularly focused on privacy issues, is necessary as it can assist students in their academic activities, personal, social, and professional life (Egelman et al., 2016).

As observed by Chang (2021), institutions need to find a balance between protecting students' privacy and violating it, which can lead to a persuasion process for those involved to step out of their "comfort zone" to share knowledge. However, stepping out of the "comfort zone" can be complex, as observed in our study, where simple processes such as guidance are still executed to a limited extent. We identified that 61.5% of students have never received guidance, manuals, guides, or other documents aimed at protecting their privacy. This result is better than the study by Freitas and da Silva (2021), where 98% of students did not receive any documentation or manual on good practices. We checked the responses from teachers and found that 40% declared that they did not receive any guidance on privacy protection. As many students seek external information regarding privacy, developing a targeted curriculum can help teachers provide practical advice to students (Egelman et al., 2016).

To increase students' and teachers' understanding of the

importance of privacy, it is essential to include this topic in the curriculum, allowing students and teachers to protect their personal data more effectively. A study by Egelman et al. (2016) indicated that college students expressed a greater desire for transparency and control over their information after receiving a three-week privacy education curriculum. Our study found that 75% of respondents consider the inclusion of privacy in the ICT curriculum "very important". However, the data also revealed that 41.8% of participants had never or rarely heard of the LGPD. That number rises to 52.8% for respondents who have never heard of the EU GDPR, highlighting the need for guidance on privacy laws in Brazil and Europe. As highlighted in the study by Vejmelka et al. (2020), there still needs to be more guidance on the process of implementing the GDPR in schools, as in Croatia and other European countries. Another challenge for people to understand privacy issues is the complexity of texts that are often difficult to comprehend, especially privacy policies (dos Reis et al., 2023).

Regarding another aspect of student privacy, we observed concerns regarding disclosing their grades. We identified that 26% of the students who responded were able to see their classmates' grades (question 25). In this case, 28% of the students had access to grades only through the system, and 35% were informed individually. The results of our study differ somewhat from those of Freitas and da Silva (2021), where 87% of students reported viewing their grades individually with login and password. This could be due to the emergency structuring for the pandemic in Brazil. Many students described difficulties in performing online activities, expressing themselves, and/or having their data exposed, as presented in question 27. This could be because anonymity is a characteristic that needs to be maintained in educational systems, as students do not feel comfortable sharing certain information (Chang, 2021).

Similarly to students, teachers also face challenges in integrating the topic of privacy into the ICT curriculum. It is essential to have a training and awareness-raising process for teachers so that they can integrate the topic into the teaching process. A study conducted in the USA noted that despite the importance of covering the topic of privacy in computer science curricula aimed at high school and undergraduates, this still needs to be done (Egelman et al., 2016).

While there are still numerous challenges to be faced by both teachers and students, it is imperative for ICT course curricula to address privacy concerns. Nevertheless, there are already some measures and practices implemented in everyday life that can be adopted in online classes to enhance privacy protection, such as guidelines on recording, storage, the intended purpose of recording, and how to preserve anonymity during recorded classes. Drawing from the data gathered in this study and the literature, we present in the 6 section a set of lessons learned that can aid in safeguarding the privacy of participants in future online teaching and learning activities.

6 Lessons Learned

This section presents some lessons learned that can assist in privacy protection during online teaching activities, which can be applied by institutions, teachers, and students. The lessons learned are based on information described in the literature, where it is observed that informing the data subject about their privacy can help them protect their data and implement good practices (Mutimukwe et al., 2022). The process of educating and preparing all parties involved to improve privacy protection during online teaching activities provides a better understanding of the risks involved, as well as the importance and responsibility of the parties involved (Ali and Zafar, 2017).

In some countries, there are already clear guidelines for protecting the privacy of students in teaching activities, such as in Portugal, where the National Data Protection Commission (CNPD) provides guidance on how teachers should proceed regarding the exposure of grades, student results, and other data (Freitas and da Silva, 2021). Educational institutions need to develop good practice structures in processes to protect the privacy of those involved in teaching, such as guiding students to use pseudonyms or IDs when identifying themselves (Alier et al., 2021). In Brazil, there is currently no specific guide to guide educational institutions, teachers, or students regarding good privacy protection practices; however, there is a good practices guide from LGPD (Brasil, 2020).

The lessons learned outlined in this section can aid in the conception and organization of good practice guides, manuals, or other forms of guidance. These lessons are derived from both literature review and our own research, and while their focus is on ICT courses, they can be applied more broadly to other educational institutions. The lessons learned are organized into three subsections: what can institution do, what can teachers do, and what can students do.

6.1 What can institutions do?

To ensure the privacy of everyone involved in the teaching process, institutions must control access to data on teaching platforms and in the means of communication used, especially in the remote teaching process, in order to protect students and teachers de Almeida et al. (2020). Portugal's National Data Protection Commission (CNPD) established a set of guidelines for the use of technologies to support distance learning while maintaining compliance with the GDPR in 2020 CNPD (2018). Similarly, UNESCO presented a guide for protecting privacy in online teaching activities aimed at teachers and students in 2020 Huang et al. (2020).

However, Brazilian data protection legislation does not cover or describe specific items related to the process of distance learning or online education de Almeida et al. (2020). The data protection guides made available by the Federal Government are still generic, such as the LGPD Good Practices Guide Brasil (2020). Therefore, each educational institution needs to structure and create its guidelines and processes aimed at ensuring protection and privacy in online teaching, guiding teachers and students. Various tools can be used for this purpose, such as guides, manuals, documenta-

tion, videos, and emails, among others, to disseminate information and guidance.

Based on the literature and data observed in our study, we identified some guidelines that educational institutions can use to protect the privacy of teachers and students. This allows everyone involved to better understand their role in protecting their data, thus improving the privacy of everyone involved.

- Disseminate information and guidance on the LGPD to all individuals connected to the institution, including students, teachers, and employees.
- Develop a transparent and accessible privacy policy that describes how personal data is used by all individuals involved in online teaching activities, including internal systems and teaching processes.
- Identify the person responsible for data protection in the institution and provide clear instructions on how to contact them.
- Create consent terms related to privacy that can be used by teachers with students at the beginning of the semester.
- Transparently and proactively communicate about any privacy-related issues or gaps that may have occurred within the institution.
- Disseminate the Personal Data Protection Impact Report and other privacy-related reports.
- Integrate discussions on privacy in relevant disciplines or courses.
- Provide guidance on:
 1. where the privacy policy is located;
 2. the location of documentation, manuals, videos, etc. related to the LGPD and its use in the institution;
 3. the risks of misusing personal data;
 4. the internal rules dealing with the protection of personal data;
 5. how to inform students/participants about the recording of teaching activities and its purpose;
 6. how to request authorization to record teaching activities and in other situations;
 7. how to proceed and communicate about the storage location and safety procedures adopted;
 8. how to inform students if their data has been deleted or the length of time that a video, audio, image, or information containing personal data will be stored;
 9. how to make students' grades and personal information available;
 10. how to proceed in relation to personal data exposed by someone from the institution; and how and for what purpose personal data of everyone involved in the teaching process may be used in the educational institution.

As noted by de Almeida et al. (2020), everyone involved in online teaching activities must commit to privacy protection, especially institutions, which should carry out activities (e.g., training, guidance, reports) to provide transparency, address privacy issues, and promote the ethical use of ICTs and responsibility for information produced.

6.2 What can teachers do?

The teacher must consider legal issues when designing a teaching activity that involves collecting, communicating, and storing student data, including online teaching activities.

Educational institutions can help teachers protect their and students' privacy by providing information on best practices for handling personal data. However, teachers can also seek guidance from literature, news, announcements, and other data to stay informed about protecting their data and that of their students.

When creating an activity that will store, whether digitally or physically, the students' data, the teacher needs to consider legal issues, being able to:

- Present a consent form related to privacy issues in an online activity or any activity that collects personal data to students.
- At the beginning of the semester, present students with the rules and procedures for how online activities will be carried out regarding privacy issues.
- Make students' grades and results available only for individual and confidential activities.
- Do not send or make personal information of students (name, grades, e-mail, etc.) available for viewing or downloading.
- Use registration numbers or other forms of data anonymization when providing results of student activities.
- Communicate when an activity is being recorded, the purpose of recording, storage time, and storage location.
- Provide an alternative link to students who do not wish to be recorded, if possible.
- Address the privacy issue in subjects that may involve the future/current use of personal data.
- Guide students on:
 1. where to locate the institution's privacy policy and manuals;
 2. how to proceed about personal data exposed by someone in the class or institution;
 3. how to avoid appearing in recordings if they do not wish to;
 4. students that class videos cannot be made available to third parties. They are for classroom use only;
 5. their rights related to the privacy of their data when carrying out online activities that involve data collection;
 6. the ethical and correct way to record classes/activities on their computers with authorization from colleagues or teachers.

6.3 What can students do?

The institution and faculty hold a responsibility to address privacy concerns, but students also bear the onus of safeguarding their personal and peer privacy. Here are some ways in which students can contribute:

- Read the privacy policy on the institution's website.

- Ask teachers for information about the rules related to privacy that apply to the course content.
- Check with the teacher about the rules governing privacy during the course, including recording, storage, and sharing of data involving students.
- Do not record or collect data from colleagues and teachers without their consent.
- Do not share private information about colleagues and teachers, even if it is related to class, with third parties.
- Observe the institution's Ethics Committee rules and relevant legislation when conducting academic research.
- Be careful when sharing information on social networks, email, and other apps to avoid sharing personal, private, or confidential information.
- Ask teachers about how they address privacy concerns related to the subject being.

7 Threats to Validity

Based on the study by Wohlin et al. (2012) on experimentation in software engineering, we have attempted to reduce threats to the validity of our study. However, we acknowledge potential threats to validity:

External Validity: Our sample size was limited to 91 respondents, which may restrict the generalizability of our results to the entire population of teachers and students in all ICT courses in public and private institutions. To mitigate this threat, we presented a detailed result and a discussion. Future studies with larger sample sizes for both quantitative and qualitative studies are planned.

Construct Validity: The generalization of the study results to other institutions, teachers, and students is a threat due to the scenario of Brazilian institutions. The survey was conducted only in Brazil, and most participants were from Rio de Janeiro and public universities. Perceptions about data privacy during teaching and learning in higher education could vary among different states of Brazil and various public and private universities. Thus, the results of this study may not be generalizable to all institutions, teachers, and students in other countries. However, we attempted to recruit a wide sample for the survey to minimize this threat.

Another threat affecting the construction validity is not submitting the survey to the Research Ethics Committee. However, this lack of submission of the study can be justified by several factors. First, it is essential to highlight the context in which the research was carried out during the COVID-19 pandemic, which imposed restrictions and operational difficulties. In addition, as part of an academic study, we had little time available to start the research, which reinforces the need for agility in conducting processes. To mitigate this threat, we ensured compliance with the ethical aspects of the study was guaranteed by sending the Free and Informed Consent Form to the participants, ensuring the transparency and autonomy of these individuals regarding their participation in the research. Furthermore, all shared data was anonymized before use.

Internal Validity: Our sample consists of different respondents, teachers, and students with varying teaching and learning experiences. Therefore, different groups of teachers and

students in different institutions may be affected by the experience of teaching and learning differently. To mitigate this threat, future works will apply proposed good practices and conduct further investigations

Regarding *Conclusion Validity:* We did not use statistical tests during the data analysis for both quantitative and qualitative studies. Therefore, we cannot conclude that there is a statistically significant difference in the results, which may be considered a threat to conclusion validity. We mitigated this threat by describing our results as indications and presenting the discussions rather than as factual conclusions.

8 Final Considerations and Future Works

In this study, we investigated how teachers and students from undergraduate and graduate ICT courses were guided on issues related to privacy in remote activities during the COVID-19 pandemic, which were conducted in 2020 and 2021. The study involved participants, students, and teachers from undergraduate and graduate ICT courses. We designed a questionnaire based on literature, which was answered by 91 participants (teachers and students) from various higher education institutions.

During data analysis, we identified some counseling practices related to privacy that teachers followed. For example, 93% of teachers ever or frequently informed students that the activity was being recorded. In contrast, 91% of students remembered that they were ever or frequently informed that the class was being recorded.

The main contributions of this study are:

(i) Identification of some guidance practices on protecting personal data that are already being adopted by teachers and students but need to be better implemented. For instance, institutions must disclose privacy policies, inform where and how long class videos will be stored, and provide general guidance on LGPD.

(ii) Based on the information collected, we identified some lessons learned that can be adopted to protect participants' privacy in online teaching-learning activities.

(iii) We identified in the responses of teachers and students several challenges that they are facing, which require greater attention from all those involved in the teaching-learning process.

One limitation of the study is that it involved a small population of teachers and students from certain regions of the country, requiring further research on this topic. This exploratory research proved to be essential, but we understand that most respondents are from the Southeast and Midwest regions of Brazil. We intend to carry out other studies with teachers and students from other regions of Brazil.

It is also necessary to examine how this process is taking place in private educational institutions, as the participants in this study were from public institutions. We did not conduct an exploratory research or an in-depth study on how the process is taking place in private institutions in Brazil.

Another limitation of this research concerns representativeness. The sample had 91 valid answers among surveyed teachers and students in Brazil. Although it represented a

good sample in this scenario, the results cannot be generalized to an international scale. Therefore, we will conduct replications in international contexts.

For future work, it is necessary to investigate other ways of guiding teachers and students better, seeking to identify ways to maintain accessible and constant communication on privacy. From another perspective, it would be pertinent to investigate how public administrators of educational institutions or those responsible for data protection position themselves on this issue.

Finally, we planned to conduct a Systematic Literature Mapping (SLM) to categorize and synthesize research on strategies for communicating, coordinating, and collaborating on data privacy using the hybrid search method (Petersen et al., 2015; Mourão et al., 2017). This method involves utilizing a Database Search in Scopus to identify pertinent initial articles, followed by parallel Backward and Forward Snowballing (Mourão et al., 2020). This hybrid search approach has shown to achieve a suitable balance between the quality of results and review effort, and the insights and analysis gleaned from this process can aid us in the subsequent stages of this research.

Acknowledgements

This study was financed in part by the Fundação de Amparo à Pesquisa do Estado do Rio de Janeiro (FAPERJ) Finance Code SEI-260003/014815/2022.

This study was financed in part by the Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – Brasil (CAPES) – Finance Code 001.

This study was financed in part by the Instituto Federal de Educação, Ciência e Tecnologia de Mato Grosso (IFMT).

We thank the volunteers that took part of the study

Notes

This manuscript is an extended version of the work “Privacidade na Educação on-line em Tempos de Pandemia: Um levantamento de práticas adotadas e possibilidades futuras”, da Silva et al. (2022b), presented in the III Workshop sobre as Implicações da Computação na Sociedade, CSBC/2022.

Conflict of Interest

The authors have no relevant financial or non-financial interests to disclose, and all authors approve the manuscript for publication and reuse of the material.

References

- Ali, R. and Zafar, H. (2017). A security and privacy framework for e-learning. *International Journal for e-Learning Security*.
- Alier, M., Casañ Guerrero, M. J., Amo, D., Severance, C., and Fonseca, D. (2021). Privacy and e-learning: A pending task. *Sustainability*, 13(16):9206.
- Balash, D. G., Kim, D., Shaibekova, D., Fainchtein, R. A., Sherr, M., and Aviv, A. J. (2021). Examining the examiners: Students’ privacy and security perceptions of online proctoring services. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 633–652.
- Basili, V. R. (1993). Applying the goal/question/metric paradigm in the experience factory. *Software quality assurance and measurement: A worldwide perspective*, 7(4):21–44.
- Basili, V. R. and Rombach, H. D. (1988). The tame project: Towards improvement-oriented software environments. *IEEE Transactions on software engineering*, 14(6).
- Boscarioli, C., DE ARAUJO, R. M., and Maciel, R. S. P. (2017). I grandsi-br grand research challenges in information systems in brazil 2016-2026. *SBC-Sociedade Brasileira de Computação*.
- Branco, E. P., Adriano, G., and Zanatta, S. C. (2020). Educação e tdic: contextos e desafios das aulas remotas durante a pandemia da covid-19. *Debates em Educação*, 12:328–350.
- Brasil (2013). Resolução nº 466, de 12 de dezembro de 2012. *Diário Oficial da União*, 12:59–59. <https://conselho.saude.gov.br/resolucoes/2012/Reso466.pdf>.
- Brasil (2016). Resolução nº 510, de 7 abril de 2016. <https://conselho.saude.gov.br/resolucoes/2016/Reso510.pdf>.
- Brasil (2018). Lei nº 13.709, de 14 de agosto de 2018. Disponível em http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. accessed in: 05/03/2022.
- Brasil (2020). Guia de boas práticas - lgp. Available in: <https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias-operacionais-para-adequacao-a-lei-geral-de-protecao-de-dados-pessoais-lgp>. Accessed in: 20/04/2023.
- Chang, B. (2021). Student privacy issues in online learning environments. *Distance Education*, 42(1):55–69.
- CNPd (2018). Orientações para utilização de tecnologias de suporte ao ensino à distância. Available in: https://www.cnpd.pt/media/1encswse/orientacoes_tecnologias_de_suporte_ao_ensino_a_distancia.pdf. Accessed in 20/11/22.
- Cristani, M., Alves, W., Pereira, G., and Lazarin, N. (2020). Um breve panorama sobre a disciplina de segurança nos cursos de sistemas de informação no brasil. In *Anais Estendidos do XVI Simpósio Brasileiro de Sistemas de Informação*, pages 1–4, Porto Alegre, RS, Brasil. SBC.
- da Silva, M., Filho, J. V., and Salgado, L. (2022a). Investigando o pensamento de docentes e discentes de cursos tic com relação à privacidade durante uso de redes sociais. In *Anais do XIII Workshop sobre Aspectos da Interação Humano-Computador para a Web Social*, pages 32–39, Porto Alegre, RS, Brasil. SBC.
- da Silva, M., Viterbo, J., Bernardini, F., and Maciel, C. (2018). Identifying privacy functional requirements for crowdsourcing applications in smart cities. In *2018 IEEE International Conference on Intelligence and Security Informatics (ISI)*. IEEE.

- da Silva, M., Viterbo, J., and de Castro Salgado, L. C. (2022b). Privacidade na educação on-line em tempos de pandemia: Um levantamento de práticas adotadas e possibilidades futuras. In *Anais do III Workshop sobre as Implicações da Computação na Sociedade*, pages 1–12. SBC.
- da Silva, M., Viterbo, J., Salgado, L. C. C., and Andrade, E. d. O. (2023). Applying semiotic engineering in game pre-production to promote reflection on player privacy. In *Information Technology and Systems: Proceedings of ICITS 2023*. Springer.
- de Almeida, A. O., Junior, A. A., Canato, R. L. C., Albardeiro, S. T., and Marques, V. C. (2020). Ética, segurança e privacidade na educação à distância durante a pandemia no brasil. *Revista InovaEduc*, (7):1–28.
- dos Reis, V. Q., Rabello, M. E., Lima, A. C., Jardim, G. P., Fernandes, E. R., and Brefeld, U. (2023). Data practices in apps from brazil: What do privacy policies inform us about? *Journal on Interactive Systems*, 14(1):1–8.
- Dragoni, N., Lafuente, A. L., Massacci, F., and Schlichtkrull, A. (2021). Are we preparing students to build security in? a survey of european cybersecurity in higher education programs [education]. *IEEE Security & Privacy*, 19(01):81–88.
- Egelman, S., Bernd, J., Friedland, G., and Garcia, D. (2016). The teaching privacy curriculum. In *Proceedings of the 47th ACM Technical Symposium on Computing Science Education*, pages 591–596.
- Fink, A. (2003). *The survey handbook*. sage, Thousand Oaks, California.
- Freitas, M. d. C. and da Silva, M. M. (2021). Gdpr and distance teaching and learning. In *2021 16th Iberian Conference on Information Systems and Technologies*, pages 1–6. IEEE.
- Gil, A. C. (2002). Como classificar as pesquisas. *Como elaborar projetos de pesquisa*, 4(1):44–45. https://www.academia.edu/6106059/Ric_CLASSIFICAPESQUISAGIL?from=cover_page.
- Gioia, R. D., Chaudron, S., Gemo, M., and Sanchez, I. (2019). Cyber chronix, participatory research approach to develop and evaluate a storytelling game on personal data protection rights and privacy risks. In *International Conference on Games and Learning Alliance*, pages 221–230. Springer.
- Gudmundsdottir, G. B., Gassó, H. H., Rubio, J. C. C., and Hatlevik, O. E. (2020). Student teachers' responsible use of ict: Examining two samples in spain and norway. *Computers & Education*, 152:103877.
- Harpe, S. E. (2015). How to analyze likert and other rating scale data. *Currents in Pharmacy Teaching and Learning*, 7(6):836–850.
- Huang, R., Liu, D., Zhu, L., Chen, H., Yang, J., Tlili, A., Fang, H., and Wang, S. (2020). Personal data and privacy protection in online learning: Guidance for students, teachers and parents. *Beijing: Smart Learning Institute of Beijing Normal University 109p*.
- Kim, S. S. (2021). Motivators and concerns for real-time online classes: focused on the security and privacy issues. *Interactive Learning Environments*, pages 1–14.
- Marković, M. G., Debeljak, S., and Kadoić, N. (2019). Preparing students for the era of the general data protection regulation (gdpr). *TEM Journal*, 8(1):150–156.
- Mourao, E., Dias, M., Pinheiro, E., Viterbo, J., and Maciel, C. (2021). Colabin: Modelo de colaboração interativa de aula fracionada para o ensino remoto na educação superior. In *Anais do XXXII Simpósio Brasileiro de Informática na Educação*. SBC.
- Mourão, E., Kalinowski, M., Murta, L., Mendes, E., and Wohlin, C. (2017). Investigating the use of a hybrid search strategy for systematic reviews. In *2017 ACM/IEEE International Symposium on Empirical Software Engineering and Measurement (ESEM)*, pages 193–198. IEEE.
- Mourão, E., Pimentel, J. F., Murta, L., Kalinowski, M., Mendes, E., and Wohlin, C. (2020). On the performance of hybrid search strategies for systematic literature reviews in software engineering. *Information and Software Technology*, 123:106294.
- Mutumukwe, C., Viberg, O., Oberg, L.-M., and Cerratto-Pargman, T. (2022). Students' privacy concerns in learning analytics: Model development. *British Journal of Educational Technology*, 53(4):932–951.
- Peng, M.-H. and Dutta, B. (2022). Impact of personality traits and information privacy concern on e-learning environment adoption during covid-19 pandemic: An empirical investigation. *Sustainability*, 14(13):8031.
- Pérez, J., Torres, R., and Von Brand, S. (2020). Cyberkids: video game for raising cyber security awareness in children. In *2020 39th International Conference of the Chilean Computer Science Society (SCCC)*, pages 1–8. IEEE.
- Petersen, K., Vakkalanka, S., and Kuzniarz, L. (2015). Guidelines for conducting systematic mapping studies in software engineering: An update. *Information and software technology*, 64:1–18.
- Prinsloo, P., Slade, S., and Khalil, M. (2022). The answer is (not only) technological: Considering student data privacy in learning analytics. *British Journal of Educational Technology*, 53(4):876–893.
- Rajab, M. H. and Soheib, M. (2021). Privacy concerns over the use of webcams in online medical education during the covid-19 pandemic. *Cureus*, 13(2).
- Regulation, P. (2016). Regulation (eu) 2016/679 of the european parliament and of the council. *Regulation (eu)*, 679:2016.
- Santino, M. and Pina, R. (2021). Professores relatam vigilância em aulas remotas na pandemia. Available in: <https://apublica.org/2021/12/professores-relatam-vigilancia-em-aulas-remotas-na-pandemia/>. Accessed in: 02/04/2022.
- Soares, H. J., Araújo, N. V. d. S., and de Souza, P. (2020). Privacidade e segurança digital: um estudo sobre a percepção e o comportamento dos usuários sob a perspectiva do paradoxo da privacidade. In *Anais do I Workshop sobre as Implicações da Computação na Sociedade*, pages 97–106. SBC.
- Sue, V. M. and Ritter, L. A. (2012). *Conducting online surveys*. Sage.
- Tahaei, M., Frik, A., and Vaniea, K. (2021). Privacy champions in software teams: Understanding their motivations,

- strategies, and challenges. In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, pages 1–15.
- Teräs, M., Suoranta, J., Teräs, H., and Curcher, M. (2020). Post-covid-19 education and education technology ‘solutionism’: A seller’s market. *Postdigital Science and Education*, 2(3):863–878.
- Vejmelka, L., Katulic, T., Jurić, M., and Lakatoš, i. M. (2020). Application of the general data protection regulation in schools: A qualitative study with teachers, professional associates and principals. In *2020 43rd International Convention on Information, Communication and Electronic Technology (MIPRO)*, pages 1463–1469.
- Villela, M. L. B., Xavier, S. I., Prates, R. O., Prates, M. O., Prates, A. A., and Cardoso, A. A. (2015). An exploratory qualitative study on people’s attitudes towards offline and online social networks: A case study at a brazilian university. *Journal on Interactive Systems*, 6(1).
- Vittorazzi, D., Araújo, N., and de Souza, P. (2019). Investigando o comportamento na web de um grupo de bacharelandos da área de tecnologia da informação. In *Anais da X Escola Regional de Informática de Mato Grosso*, pages 67–72. SBC.
- Wohlin, C., Runeson, P., Höst, M., Ohlsson, M. C., Regnell, B., and Wesslén, A. (2012). *Experimentation in software engineering*. Springer Science & Business Media.