Contemporary Educational Technology, 2023, **15**(1), ep399
ISSN: 1309-517X (Online)

OPEN ACCESS

Research Article

Pre-service teachers' perceptions of data protection in primary education

Norma Torres-Hernández [1*]
0000-0003-4744-0313

María-Jesús Gallego-Arrufat [1]
0000-0002-2296-5431

[1] Faculty of Education, University of Granada, Granada, SPAIN
[*] Corresponding author: normath@ugr.es

Citation: Torres-Hernández, N., & Gallego-Arrufat, M.-J. (2023). Pre-service teachers' perceptions of data protection in primary education. *Contemporary Educational Technology, 15*(1), ep399. https://doi.org/10.30935/cedtech/12658

ARTICLE INFO

Received: 30 May 2022

Accepted: 20 Oct 2022

ABSTRACT

The protection of personal data and privacy are important issues closely related to use of social media, information and communication technologies, and the Internet in the area of education. The treatment of academic information and use of tools and programs for instruction, communication, and learning have revealed the handling of a significant volume of personal data from different sources. It is essential to protect this information from possible privacy violations. This descriptive study, which is of transversal nonexperimental design, focuses on how 384 pre-service teachers' enrolled in educational technology courses in their education programs view the protection of personal data. The goals are to describe and analyze how these teachers perceive the risks associated with protection of data on the Internet and what they know about protection of data in primary education. We administered a questionnaire within the framework of an educational activity that focused on digital competence in data protection in education. The results show a high perception of risk in topics such as accepting cookies when surfing the Internet or transferring banking information. The knowledge the students claim to have shown a lack of information on the protection of minors' data in issues related to the development and schooling of primary school students, as well as their health, background, and family environment. Curricular treatment of these areas that includes content, practices on regulations, and adopts a situated, critical, and responsible approach in pre-service teacher education is recommended.

Keywords: data protection, pre-service teacher education, pre-service teachers, primary education, privacy

INTRODUCTION

The digital society is a hyperconnected space thanks to constant use of social media, the Internet, and information and communication technologies. Such permanent connection involves new and varied challenges for data protection and requires users increasingly to attend to information security risks, as personal data can be exposed in ways beyond their control (Cobo, 2019; Orellana, 2017; Piñar, 2020). This situation, together with the risk of massive treatment of personal data, generates great concern among the Internet users (Marín et al., 2021). Due to its repercussions for various areas of social life, protection of personal data and privacy is a topic of current importance not only in law but also in education and other areas of social life, such as economics, medicine, and technology.

Concern for protection of data and privacy in the education sector mirrors concern observed in various other sectors of society (Jones et al., 2020; Markos et al., 2017; Schomakers et al., 2019). Because this topic is currently of social interest, our study aims to provide a general overview of what pre-service teachers know about the protection of data and privacy in education. It reports their perceptions as users of the risk involved in some of their common practices on the Internet in which personal data are collected, treated, or transferred

to third parties, or privacy is violated. The study also contributes to understanding why those who must protect students' data and who will teach students to manage information properly to comply with the law need information and training about this topic.

We understand personal data as any information that identifies an individual or makes them identifiable. Personal data take different forms: numbers, characters, symbols, images, electromagnetic waves, and information from sensors and sounds (Kitchin, 2014). In digital environments, data become information generated by a variety of actions. Through the tracking, collection, and trade of data from people who either search or disseminate information online, data acquire considerable commercial value (Bodle, 2016).

The General Data Protection Regulation (European Union, 2016) understands personal data as all information about a physical person that may be identified or identifiable. The data may refer to person's name, identification number, birth date, address, or any element of physical, physiological, genetic, psychological, economic, cultural, or social element (among others) located on the Internet or in paper documents.

In the case of education, each student is a source of data of incalculable value. In a fraction of a second, someone can monitor the searches the student performs on the Internet and even how that student thinks and what they want to learn. Some studies indicate that the data gathered in educational digital environments are infinite and generate a significant quantity of unexpected correlations that make students a rich source of personal data (Jones & Regner, 2016; Kerres, 2020).

The 2018 report on the digital society in Spain (Martín et al., 2019) indicates that the population is especially concerned about privacy of personal data on the Internet and that young people show lower awareness of the privacy of their data. In the wake of the COVID-19 pandemic, Rodríguez et al. (2021) consider a series of skills related to privacy, management, and personal data analysis to be necessary components of a set of *foundational skills* for work life in the digital society. Because many practices in today's society are mediated by technology, it is necessary to promote the development of digital competence to act in the different spheres of a person's life (Bartrina, 2014) in ways that care for and protect their personal data.

In addition to data treatment itself, use of the Internet and social media–typically employed in the educational environment–is closely linked to data protection. According to Troncoso (2010), social media enable the generation of interest groups based on personal data. Studies such as Marín et al. (2021) argue, however, that pre-service teachers have little knowledge about privacy of data and social media.

The risks and problems associated with privacy, data protection, and intellectual property are not isolated questions when technology and the Internet are used for school. Following Torres-Hernández and Gallego-Arrufat (2022), technology use in education for administrative, teaching, and research purposes requires attention to regulations in these matters and the proposal of preventive and educational actions for both *in-service* and *pre-service* teachers.

The digital society as a whole and the area of education in particular are very concerned about this topic, and the literature is gradually beginning to consolidate a body of research that treats personal data in education. We still lack considerable knowledge, however, about the implications of the recording, treatment, and communication of personal data in education. Digital education must involve not only acquiring knowledge but also knowing how to apply that knowledge and to act in various situations in which the confidentiality of information or personal data could be violated.

The area *protecting personal data and privacy* in the European framework for the educational environment [DigCompEdu] (Redecker, 2017) demands specific digital competence in matters of data protection in digital environments. This competence is necessary to take measures to protect confidential data and resources (e.g., students' grades, exams, etc.) and to share administrative information, such as data on classmates, students, and their families, as well as personal information.

If we examine regulation of data protection in the European and Spanish context, both the General Data Protection Regulation (GDPR) (European Union, 2016) and Spain's Organic Law for Protection of Data and Guarantee of Digital Rights (*Ley Orgánica de Protección de Datos y Garantía de Los Derechos Digitales* [LOPDGDD]) (Ley Orgánica, 2018) provide directives to protect the data of natural persons, but they do not provide clear lines about data treatment in education. More specifically, Article 83 of the legislation known as LOPDGDD

includes the stipulation that study programs for university degrees–especially professional degrees–guarantee education of students in the use and security of digital media and in the guarantee of fundamental rights on the Internet. The article mentions that education administrations should pay special attention to risk situations arising from inappropriate use of the Internet. It also refers to the obligation to provide training in data protection and to improve teachers' digital competence for teaching.

Prior antecedents show the need for and importance of having all education professionals know, apply, and respect in practice what is required to protect data and privacy in education (Gallego-Arrufat et al., 2019). These professionals must also explicitly promote behavior and attitudes for responsible use of social media, information and communication technologies, and the Internet (Dodel & Mesch, 2018; Fernández-Cruz & Fernández-Díaz, 2016; Forbes, 2017; Yan, 2009). It is crucial to make pre-service teachers aware which activities may be considered punishable and to ensure that these teachers know how and when to act and report actions that violate the data protection, privacy, and intimacy of students or any other member of the educational community. This demand can be met with training in the fields of educational technology in higher education, training that involves less merely instrumental use and more critical use and active commitment (Castañeda & Selwyn, 2018).

Some studies, such as that by Pangrazio and Selwyn (2019), argue the importance of data protection and propose a critical framework in which education must play a decisive role, while Wissinger (2017) considers literacy in privacy as a process of critical thinking, not a process of rule-based learning. Studies that develop a literacy focus for minors in privacy-based matters within the framework of contextual integrity (e.g., Kumar et al., 2020) or a program of educational activities in pre-service teacher education (Torres-Hernández et al., 2019) are thus of great interest for this study.

As to pre-service teachers' knowledge and practice related to data protection, we find some studies in the literature on data protection in pre-service teacher education. Gudmundsdottir et al. (2020) focus their study on the dimension of privacy that pre-service teachers must acquire for technology use and teaching. Jones (2019) concludes that university students reveal data and information to the institution and third parties in many ways. Marín et al. (2021) find that pre-service teachers have little ability to control these revelations. It is thus necessary to have better self-control of the data themselves (Kay & Kummerfeld, 2019). In evaluating the level of knowledge, practice, and attitudes toward data protection, Napal et al. (2018) find that persons currently trained to be teachers show a basic level on the topic of personal data protection. For Auxier et al. (2019), realizing that people have only slight knowledge of privacy is important evidence, as it can help people protect their privacy through education.

These antecedents provide information on the importance of data protection, low levels of pre-service teachers' competence in these matters, and the need for education to provide frameworks for protection beyond the de facto recognition that occurs around practices or knowledge of personal data protection.

Research Questions

1. **RQ1.** What level of risk do pre-service teachers perceive in practices that involve transfer of personal data?
2. **RQ2.** What knowledge do the pre-service teachers claim to have related to treatment of personal data in primary education?

METHODOLOGY

The study is descriptive and uses a quantitative methodology with cross-sectional, non-experimental design. Its goals are to describe and analyze how pre-service teachers perceive the risks (goal 1) and describe and analyze their knowledge concerning data protection in primary education (goal 2).

Participants

The study sample was composed of 384 pre-service teachers chosen by convenience sampling from natural groups. By gender, the sample contained 76% women and 23.4% men, ages 18-28, with the predominant age groups between 19 and 21 years of age, as shown in **Figure 1**.

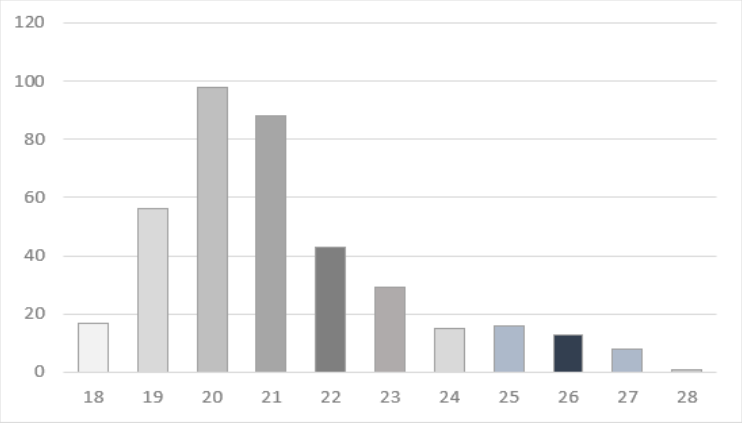


Figure 1. Ages of the pre-service teacher participants (Source: Authors)

Instrument

We used a questionnaire designed to measure risks and beliefs about data protection in education (**Table 1**). The questionnaire was composed of 31 items divided into two sections and nine subsections. The first section, *perception of risk concerning practices on the Internet that expose personal data* includes 15 items to evaluate the perception of risk in practices performed when pre-service teachers use the Internet. The responses to these questions were gathered using a Likert-type scale. The second part, *knowledge primary education teachers claim to have of practices for data protection*, contains 16 items and investigates the knowledge considered necessary for teachers in their professional practice in schools. The response options for this section were dichotomous (yes/no) plus one multiple choice option.

The questionnaire was constructed through a process of literature review and analysis of the specific relevant education legislation and documents on data protection in schools from the Spanish Data Protection Agency. We validated the questionnaire by eliciting the judgment of 12 experts who knew the material and had expertise in pre-service teacher education in subjects related to technology and education. We examined reliability and validity using different statistical analyses and obtained an acceptable total adjusted validity coefficient (CVCtc=.86) and a good Cronbach's alpha (α=.91) for reliability.

Data Collection and Analysis

The questionnaire was administered in five online workshops on protection of personal data in education, conducted in several EdTech courses in pre-service teacher training across three different academic years.

The corresponding section on perception of risks was administered to participants at the start of the educational activity as a starting point for performing the activities they were to carry out during the workshop. The section on specific knowledge of data protection in primary education was administered as initial activity in a practical case in which the pre-service teachers had to have knowledge about publication of a minor's personal information in a school.

A descriptive analysis was performed considering the number of valid cases for the mean, frequency, and standard deviation, using the following digital tools: LimeSurvey to collect the information, Excel to export the data, and SPSS for the statistical analyses.

RESULTS

The following presents the results for each of the research questions, which correspond to the two sections of the questionnaire.

RQ1. Risk Perception of Data Protection

Goal 1 focuses on describing the level of risk the pre-service teachers perceive in practices in which they transfer personal data. This goal corresponds to the questions posed in section 1 of the questionnaire (*perception of risk concerning practices on the Internet that expose personal data*).

Table 1. Structure of the questionnaire

Sections	Subsections	n	Items & codes
Section 1. Perception of risk concerning practices on the Internet that expose personal data	1.1. Concern because others have access to personal data	4	Risk of blackmail due to exposure of personal data (PR1) Loss of device with personal information (PR7) Losing control of data, not knowing their destination & use when I have profiles open on apps, tools, or programs (PR12) Publishing personal information or misinterpreting what is public (PR14)
	1.2. Sharing of data requested through the Internet	7	Accepting cookies to keep surfing (PR3) Accepting privacy policies without reading them when you register on a social media or app or when you create email accounts or use online tools (PR4) Sharing passwords for starting a session on my computer or cell phone with other people (PR6) Not knowing how the various companies manage & share my personal data (PR8) Connecting my devices on public Wi-Fi networks (PR9) Availability of the information published & posted by third parties (Facebook, WhatsApp, Instagram) so that other people–usually my online friends–can interact with the information & use it without my consent (PR10) Deactivating GPS or cell phone locator to preserve my privacy (PR15)
	1.3. Use of data for bureaucratic procedures, transactions, or contests	3	Accessing pages for betting, casinos, or online gaming in which registering requests bank account or credit card numbers (PR2) Sharing personal information or data (name, age, telephone number, credit card data, location, place of study, work-related data) that may be used by others to harm me (PR5) Filling out registration forms or personal profiles or participating in online contests on unfamiliar sites (PR11)
	1.4. Sharing of data & personal information without consent of those affected	1	Sharing & disseminating private messages to social media contacts or groups (PR13)
Section 2. Knowledge primary education teachers claim to have of data protection practices	2.1. Responsibility for treatment	1	Who is responsible for treatment of students' personal data in education? (DCP6)
	2.2. Information & consent	3	When personal data are collected on students or their families, must one inform the interested parties? (DCP5) May pre-service teachers use personal data from students in their own university papers? (DCP7) May one communicate the data to institutions, entities, or companies that the students will visit for an extracurricular activity, such as an exhibit, a museum, a factory, or a sports club? (DCP8)
	2.3. Types of students' personal data that may be shared	5	May a teacher share information on students' background or family environment? (DCP1) May a teacher share information on students' development & school performance? (DCP2) May a teacher share information related to students' health? (DCP3) May a teacher share information related to students' or their families' religious beliefs? (DCP4) In cases of gender violence, may the legal guardian oppose publication of a student's admission to a school? (DCP9)
	2.4. Publication of data on the Internet	5	May teachers record images of students or participants in a course or workshop & disseminate them via instant messaging applications? (DCP12) May one publish students' grades on a school's webpage or bulletin boards? (DCP13) May teachers publish institutional information or information about students or photos of them in their blogs? (DCP14) May one publish data from teachers, tutors, or others in charge of schools on the school's webpage? (DCP15) May one publish information about students, such as photos or videos, on the school's webpage? (DCP16)
	2.5. Use of non-institutional apps	2	May teachers create groups for instant messaging with students using applications that do not belong to the school's educational platforms? (DCP10) May teachers create groups with instant messaging applications in which parents of students in their class are members? (DCP11)

Note. n: Number of items

This section stresses the high perception of risk in Items PR3, PR2, PR7, and PR4, highlighting the agreement recorded in Item PR3, on accepting cookies when surfing the Internet. A total of 205 participants assigned this risk the highest value on the scale.

Table 2. Risk perception of pre-service teachers concerning data protection

Item-code	Not risky (1)	Slightly risky (2)	Quite risky (3)	Very risky (4)	Too risky (5)	M	SD
PR3	2.1%	8.3%	19.5%	16.7%	53.4%	4.11	1.114
PR2	2.1%	3.4%	18.8%	23.2%	52.6%	4.21	.996
PR7	1,6%	4.9%	15.4%	29.2%	49.0%	4.19	.948
PR4	2.1%	7.8%	18.8%	24.5%	46.9%	4.06	1.075
PR5	1.9%	9.9%	25.5%	26.3%	36.5%	3.86	1.162
PR12	1.8%	4.4%	29.9%	28.9%	35.4%	3.92	.985
PR14	1.8%	4.4%	29.9%	28.9%	35.4%	3.92	.985
PR11	.3%	8.3%	28.6%	28.9%	33.9%	3.88	.9.69
PR15	2.9%	6.5%	26.6%	30.7%	33.3%	3.85	1.048
PR13	2.9%	6.5%	26.6%	30.7%	33.3%	3.85	1.048
PR9	2.6%	12.8%	25.8%	25.8%	33.1%	3.74	1.126
PR8	3.9%	13.8%	33.1%	20.8%	28.4%	3.56	1.152
PR10	2,6%	17.7%	30.7%	24.0%	25.0%	3.51	1.124
PR6	4.9%	21.4%	25.8%	22.9%	25.0%	3.42	1.213
PR1	4.9%	19.8%	33.9%	22.4%	19.0%	3.31	1.289

Note. M: Mean & SD: Standard deviation

Table 2 includes results from each of the items, ordered from highest to lowest risk (from "too much" to only "quite"). **Table 2** shows the mean and standard deviation for each of the items.

The results demonstrate that the pre-service teachers perceive 73% of the total number of items to be too risky in the following practices: accepting cookies to keep browsing (53.4%); giving bank data when accessing pages for betting, casinos, or online gaming (52.6%); losing devices with personal information (49%); accepting privacy policies without reading them first (46.9%); sharing personal information that can be used to cause damage (36.5%); losing control of data when one keeps profiles open on applications and online tools (35.4%); publishing personal information and misinterpreting what is publishable (35.4%); completing registration forms or personal profiles or participating in online contests on unknown webpages (33.9%); geolocation through GPS if it is not deactivated (33.3%); sharing and disseminating private or group messages on social media (33.3%); and connecting devices to public Wi-Fi networks (33.1%).

The practices that most of the pre-service teachers perceive as considerably risky are not knowing how companies manage personal data (33.1% of total responses), having personal information that others have posted to the Internet published on social media and having this information used without their consent (PR10, 30.7%), sharing passwords with other people (25.8%), and being vulnerable to the risk of blackmail due to exposure of personal data (33.9%).

RQ2. Knowledge of Data Protection in Primary Education

Goal 2 is to describe and analyze the pre-service teachers' knowledge of data protection in primary education. This goal corresponds to the questions posed in the section on knowledge primary education teachers claim to have of practices for data protection.

Next, we present the results for each of the subsections in this section of the questionnaire.

Responsibility for treatment

Figure 2 represents the pre-service teachers' responses to the question of who was responsible for treatment of students' personal data in primary education.

The data show that 296 pre-service teachers (77%) think that all three agents involved in primary education bear responsibility: the school, the teachers, and the educational administration itself: 56 pre-service teachers believe that the school is responsible for managing the students' data (14.6%), 24 believe that the education administration is responsible (6.3%), and only 8 (2.1%) participants believe that the teachers themselves are responsible.

Figure 3 plots the behavior of the responses for each item in the remaining subsections concerning pre-service teachers' knowledge of data protection in primary education. The results are presented in order from degree of positive to degree of negative response, that is, from items with the most to items with the fewest "yes" responses, followed by the items from the fewest to items with the most "no" responses.

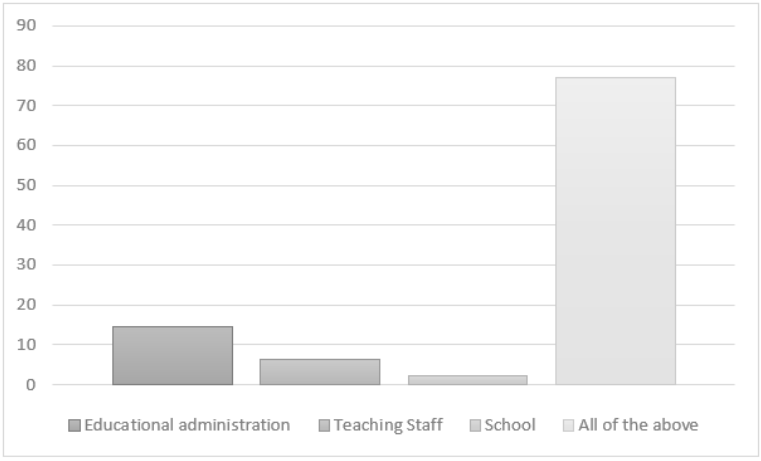
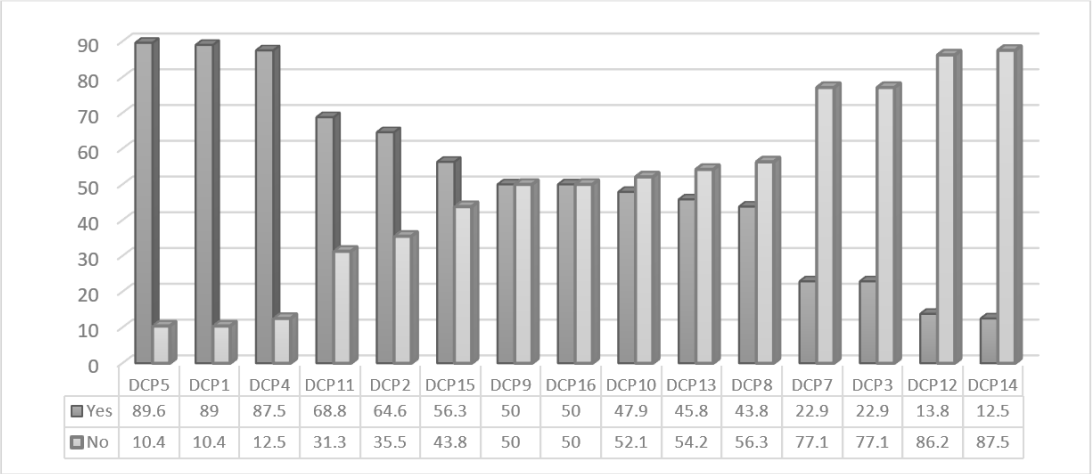


Figure 2. Responsibility for treatment of personal data, according to the pre-service teachers (Source: Authors)



	DCP5	DCP1	DCP4	DCP11	DCP2	DCP15	DCP9	DCP16	DCP10	DCP13	DCP8	DCP7	DCP3	DCP12	DCP14
Yes	89.6	89	87.5	68.8	64.6	56.3	50	50	47.9	45.8	43.8	22.9	22.9	13.8	12.5
No	10.4	10.4	12.5	31.3	35.5	43.8	50	50	52.1	54.2	56.3	77.1	77.1	86.2	87.5

Figure 3. Results obtained on the second section of the questionnaire (Source: Authors)

What situations do the pre-service teachers consider as correct when treating students' personal data? Of the total responses, 89.6% claim that they know they should inform interested parties when they gather personal data on students or their families, and 89% answer that as teachers they may share information about the student's family origin and environment. Further, 87.5% state that they may share information about students' religious beliefs, 68.8 % that they may create groups with instant messaging apps in which parents of students in the class may participate, 64.6% believe they know a teacher may share information about the student's development and school results, and 56.3% believe that they may publish data on the web on the school's teachers, guardians, or other personnel.

As to responses on knowledge concerning the right of parents or guardians to oppose publication of information from school admissions lists in situations of gender violence (DCP9) and the publication of pictures, videos, or other information on students (DCP16), the pre-service teachers answered 50% "yes" and 50% "no." When the pre-service teachers were asked whether one may organize instant messaging groups with students using applications not included on the school's educational platforms, 52.1% stated that one may not do so (DCP10). 54.2% know that one may not make students' grades public on school webpages or bulletin boards (DCP13). 56.3% state that one may not communicate data to institutions, entities, or companies that students will visit for an extracurricular activity (DCP8).

The same proportion of pre-service teachers (77.1%) knows that they may not use students' personal data gathered during their practicums in their own university projects (DCP7) and may not share information about students' health (DCP3). 86.2% of respondents claimed that they know a teacher may not record images of students or participants in a course or workshop and disseminate them through instant messaging

applications (DCP12). 87.5% know that they may not publish institutional information, information about students' exams, or pictures of students on their blog (DC14).

SUMMARY AND DISCUSSION

This article focuses on description and analysis of both pre-service teachers' perception of risks in a series of common internet practices and the knowledge these teachers claim they possess concerning treatment of personal data in primary education.

According to the results obtained, the practices for which the pre-service teachers perceived the greatest risk involve accepting cookies when browsing the Internet and sharing bank data when engaged in gaming or accessing websites for betting or online casinos. When analyzing the results in the first part of the questionnaire, the pre-service teachers perceived the greatest risk when they accept privacy policies without reading them first, share passwords with third parties, do not know how companies will treat their data, connect to public Wi-Fi, and have their location detected through a geolocator on the cell phone, GPS, or Bluetooth. Their perception of risk also increases when they lose a USB drive, keep accounts and profiles open on several devices, publish profiles on social media, and expose personal data. Their risk increases in these cases due to fear of blackmail or extorsion through their cell phone or email. As to accepting privacy policies without reading them first, 46.9% in this study perceived this behavior as risky. In Marín et al. (2021), 72.3% of the sample of pre-service teachers responded they had never read the privacy policies.

In this study, 33.1% of the pre-service teachers perceived the risk involved in companies' use and treatment of their data as lower than that recorded in Marín et al. (2021), where around 80% of the sample indicated that they felt uncomfortable with the way companies' used their data. As to knowing about data protection in primary education, some responses agreed with the obligation to inform interested parties when one collects any type of personal data. As to both risk perception and knowledge of the treatment of personal data in education, we can conclude that the pre-service teachers are aware of risks and problems that exist on the Internet.

There are results, however, that show only a basic level of knowledge concerning the categories of data that European and Spanish legislation consider as sensitive, such as information about religious beliefs, data on family origin and environment, use of noninstitutional applications to communicate with parents, sharing information about the student's school, or publishing data on teachers, homeroom teachers, or other school personnel. Our study disagrees with Marín et al. (2021), who find that pre-service teachers do not feel familiar with the applicable laws. In our study, the pre-service teachers stated that they have basic knowledge of Spanish law on education and matters of data protection that apply to the use of students' data during practicums, the prohibition against using noninstitutional messaging with students, the place to make public students' grades, knowledge about communicating data to third parties, and sharing data on students' health.

We know that no content in any course during pre-service training focuses specifically on protection of personal data in pre-service teachers' study programs. Giaever et al. (2016) indicate that countries like Norway train teachers in topics such as netiquette, cyberbullying, ethical and moral aspects of cyber ethics, and respect for copyright. Our study shows, however, that teachers have little knowledge of issues associated with privacy and encounter some difficulty teaching these issues to their students. We thus stress the importance of not accepting mere possession of specific knowledge. It is also crucial to know how to apply this knowledge and how to act in various situations in which protection of information or personal data may be violated in education.

We believe it is necessary to adopt a critical, responsible approach to technology use in training pre-service teachers–an approach like those proposed by Castañeda and Selwyn (2018), Dodel and Mesch (2018), Fernández-Cruz and Fernández-Díaz (2016), Forbes (2017), and Yan (2009). We also believe an urgent need exists to attend to questions related to data protection and privacy in the digital society, as Marín et al. (2021) indicate. If we do not develop competences in matters of data protection and privacy in pre-service teachers, their beliefs and attitudes toward technology use could become barriers to innovation and instruction. In clicking privacy policies and cookies, completing forms, and deciding whether or not to register on educational and communication applications, pre-service teachers implicitly accept that they are providing all kinds of

personal data in exchange for supposed ease, sheltered by their belief in the myth that computer security is inviolable.

The digital immersion experienced by much of the population during the COVID-19 pandemic increased awareness in various sectors that we must take care to prevent against large-scale capture of data and information. *Data culture* is a current phenomenon that helps us to reflect on how we value our data. An important dilemma that education faces, however, is that technology both provides a great number of advantages and generates quantities of data that were unthinkable years ago. Given this practice, educators face greater fragility in their efforts to protect data, due largely to lack of preparation. Pre-service teachers are also concerned because their day-to-day training requires use of educational platforms or tools in which they must risk their personal data or accept cookies.

Given the various problems due to improper use of personal data and privacy that also affect the education sector, it is important to note that responsible use requires pre-service teachers to go beyond merely accepting and stating that they are competent or concerned about privacy. It is crucial that they know how to apply their knowledge and act in various situations in education in which protection of information or personal data may be violated. Studies cited above (Giaever et al., 2016; Gudmundsdottir et al., 2020) point to the minimal information on these issues, information that would enable the pre-service teachers to understand better what questions are in play, which are applied, and which are not problematic. Marín et al. (2021) indicate that teachers' information is crucial and that literacy on privacy must be included in the design of education as instructional strategy and curricular content during pre-service training. We thus agree with conclusions from prior research on the importance of educating and raising the awareness of pre-service teachers. Such education will enable them to know what practices may be punished, as well as precisely when and how to act to counter any action that violates data or privacy and affects members of the community, as indicated in Gallego-Arrufat et al. (2019).

This study focuses on the higher education institutions that train pre-service teachers and the importance of curricular treatment of data protection in university education, as shown in the results of this study, which aligns with other research contributions (Gudmundsdottir et al., 2020; Giaever et al., 2016; Marín et al., 2021). We thus propose incorporating education content and practicums on data protection into pre-service training, based on a critical and responsible approach to technology use that contributes to decreasing concern about the high exposure of personal data and care for privacy in education. Attention to these questions requires urgent attention. They form part of the challenges of the digital society and require real practices and committed approaches, in which digital education plays a determining role.

Future Lines of Research

1. We propose the need for more in-depth study of how higher education institutions responsible for pre-service training are incorporating questions associated with protection of personal data and privacy into Education study programs.
2. Based on the results of this study and those of Marín et al. (2021), which focus on privacy and cookies policies, we propose research on the possible association between effective reading and perception of risk in protecting the personal data gathered by applications used in the educational environment.
3. Another interesting line of research that emerges from this study is analysis of the relationship between pre-service teachers' knowledge and the risks they perceive in practices where they put into play different types of personal data.

Author contributions: All authors were involved in concept, design, collection of data, interpretation, writing, and critically revising the article. All authors approve final version of the article.

Funding: This article was supported by Spanish Ministry of Education & Vocational Training (Reference: FPU17/05164).

Ethics declaration: The authors declared that the study was conducted in accordance with the Declaration of Helsinki and the Code of good practice in research approved by the University of Granada, Spain. Vice-Rectorate for Research and Knowledge Transfer. http://sl.ugr.es/0cgh. Informed consents were obtained from the participants. Anonymity of the personal data have been protected.

Declaration of interest: Authors declare no competing interest.

Data availability: Data generated or analyzed during this study are available from the authors on request.

REFERENCES

Auxier, B., Rainie, L., Anderson, M., Perrin, A., Kumar, M., & Turner, E. (2019). Americans and privacy: Concerned, confused, and feeling lack of control over their personal information. *Pew Research Center: Internet, Science, & Tech*. https://policycommons.net/artifacts/616499/americans-and-privacy/1597152/

Bartrina, M. J. (2014). Cyberbullying behavior in children and adolescents: Education and social awareness as a way out. *Educar, 50*(2), 343-400. https://doi.org/10.5565/rev/educar.672

Bodle, R. (2016). A critical theory of advertising as surveillance. Algorithms, big data, and power. In J. F. Hamilton, R. Bodle, & E. Korin (Eds.), *Explorations in critical studies of advertising* (pp. 138-152). Routledge.

Castañeda, L., & Selwyn, N. (2018). More than tools? Making sense of the ongoing digitization of higher education. *International Journal of Educational Technology in Higher Education, 15*, 22. https://doi.org/10.1186/s41239-018-0109-y

Cobo, C. (2019). *Acepto las condiciones. Usos y abusos de las tecnologías digitales* [*I accept the conditions. Uses and abuses of digital technologies*]. Fundación Santillana.

Dodel, M., & Mesch, G. (2018). Inequality in digital skills and the adoption of online safety behaviors. *Information, Communication & Society, 21*(5), 712-728. https://doi.org/10.1080/1369118X.2018.1428652

European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation, GDPR).* https://bit.ly/3CxIGdB

Fernández-Cruz, F. J., & Fernández-Díaz, M. J. (2016). Generation Z's teachers and their digital skills. *Comunicar, 46,* 97-105. https://doi.org/10.3916/C46-2016-10

Forbes, D. (2017). Professional online presence and learning networks: Educating for ethical use of social media. *The International Review of Research in Open and Distributed Learning, 18*(7), 175-190. https://doi.org/10.19173/irrodl.v18i7.2826

Gallego-Arrufat, M.J., Torres-Hernández N., & Pessoa, T. (2019). Competence of future teachers in the digital security area. *Comunicar, 61*, 57-67. http://doi.org/10.3916/c61-2019-05

Giaever, T., Mifsud, L., & Gjolstad. (2016). *Teachers' understanding and practice of cyber ethics in the classroom* [Paper presentation]. The 9th Annual International Conference of Education, Research, and Innovation. https://doi.org/10.21125/iceri.2016.0421

Gudmundsdottir, G. B., Hernández, H., Colomer, J. C., & Hatlevik, O. E. (2020). Student teachers' responsible use of ICT: Examining two samples in Spain and Norway. *Computers & Education, 152*, 103877. https://doi.org/10.1016/j.compedu.2020.103877

Jones, K. M. L. (2019). Learning analytics and higher education: A proposed model for establishing informed consent mechanisms to promote student privacy and autonomy. *International Journal of Educational Technology in Higher Education, 16*, 24. https://doi.org/10.1186/s41239-019-0155-0

Jones, K. M. L., Asher, A., Goben, A., Perry, M. R., Salo, D., Briney, K. A., & Brooke, M. B. (2020). "We're being tracked at all times:" Student perspectives of their privacy in relation to learning analytics in higher education. *The Journal of the Association for Information Science and Technology, 71*(9), 1044-1059. https://doi.org/10.1002/asi.24358

Jones, M. L., & Regner, L. (2016). Users or students? Privacy in university MOOCS. *Science and Engineering Ethics, 22*, 1473-1496. https://doi.org/10.1007/s11948-015-9692-7

Kay, J., & Kummerfeld, B. (2019). From data to personal user models for life-long, life-wide learners. *British Journal of Educational Technology, 50*(6), 2871-2884. https://doi.org/10.1111/bjet.12878

Kerres, M. (2020). Against all odds: Education in Germany oping with COVID-19. *Postdigital Science and Education, 2*, 690-694. https://doi.org/10.1007/s42438-020-00130-7

Kitchin, R. (2014). *The data revolution: Big data, open data, data infrastructures & their consequences*. SAGE. https://doi.org/10.4135/9781473909472

Kumar, P. C., Subramaniam, M., Vitak, J., Clegg, T. L., & Chetty, M. (2020). Strengthening children's privacy literacy through contextual integrity. *Media and Communication, 8*(4) 175-184. https://doi.org/10.17645/mac.v8i4.3236

Ley Orgánica de protección de datos y garantía de los derechos digitales [Organic Law on Data Protection and Guarantee of Digital Rights]. [LOPDGDD] (2018). Head of State. *Official State Gazette*, 294, 119788-119857. https://www.boe.es/buscar/pdf/2018/BOE-A-2018-16673-consolidado.pdf

Marín, V. I., Carpenter, J. P., & Tur. G. (2021). Pre-service teachers' perceptions of social media data privacy policies. *British Journal of Educational Technology, 52*(2), 519-535. https://doi.org/10.1111/bjet.13035

Markos, E., Milne, G. R., & Peltier, J. W. (2017). Information Sensitivity and Willingness to Provide Continua: A Comparative Privacy Study of the United States and Brazil. *Journal of Public Policy & Marketing, 36*(1), 79-96. https://doi.org/10.1509/jppm.15.159

Martín, J. M., Suero, C., Suso, A., & Torres, J. (2019). *Sociedad digital en España, 2018* [*Digital society in Spain, 2018*]. Taurus/Fundación Telefónica.

Napal, M., Peñalva-Vélez, A., & Mendióroz, A. (2018). Development of digital competence in secondary education teachers' training. *Education Sciences, 8*, 104. https://doi.org/10.3390/educsci8030104

Orellana, C. (2017). De la seguridad cibernética a la resiliencia cibernética aplicada a la protección de datos personales [From cyber security to cyber resilience applied to personal data protection]. *Revista de Derecho* [*Law Magazine*]*, 27*, 5-23. https://core.ac.uk/download/pdf/159773911.pdf

Pangrazio, L., & Selwyn, N. (2019). 'Personal data literacies': A critical literacies approach to enhancing understandings of personal digital data. *New Media & Society, 21*(2), 419-437. https://doi.org/10.1177/1461444818799523

Piñar, J. L. (2020). Derecho e innovación: Privacidad y otros derechos en la sociedad digital [Law and innovation: Privacy and other rights in the digital society]. In M. E. Casas (Ed.), *El derecho a la protección de datos personales en la sociedad digital* [*The right to personal data protection in the digital society*] (pp. 39-63). Fundación Ramón Areces.

Redecker, C. (2017). *European framework for the digital competence of educators: DigCompEdu*. In Y. Punie (Ed.), *Publications Office of the European Union*. Joint Research Centre No. JRC107466. https://doi.org/10.2760/178382

Rodríguez, P., Villas, J., Tarín, X., & Blázquez, S. (2021). *Sociedad digital en España. El año que todo cambió* [*Digital society in Spain. The year everything changed*]. Fundación Telefónica. https://www.fundacion telefonica.com/cultura-digital/publicaciones/sociedad-digital-en-espana-2020-2021/730/

Schomakers, E., Lidynia, Ch., Müllmann, D., & Ziefle, M. (2019). Internet users' perceptions of information sensitivity – insights from Germany. *International Journal of Information Management, 46*, 142-150. https://doi.org/10.1016/j.ijinfomgt.2018.11.018

Torres-Hernández, N., & Gallego-Arrufat, M. J. (2022). Indicators to assess preservice teachers' digital competence in security: A systematic review. *Education and Information Technologies, 27*, 8583-8602. https://doi.org/10.1007/s10639-022-10978-w

Torres-Hernández, N., Gallego-Arrufat, M. J., & Pessoa, T. (2019). Intervention and e-assessment with technologies of the competence in digital security. *Digital Education Review, 35*, 111-129. https://doi.org/10.1344/der.2019.35.111-129

Troncoso, A. (2010). *La protección de datos personales. En busca del equilibrio* [*The protection of personal data. In search of balance*]. Tirant Lo Blanch.

Wissinger, C. L. (2017). Privacy literacy: From theory to practice. *Communications in Information Literacy, 11*(2), 378-389. https://doi.org/10.15760/comminfolit.2017.11.2.9

Yan, Z. (2009). Differences in high school and college students' basic knowledge and perceived education of Internet safety: Do high school students really benefit from the children's internet protection act? *Journal of Applied Developmental Psychology, 30*(3), 209-217. https://doi.org/10.1016/j.appdev.2008.10.007