education policy analysis archives

A peer-reviewed, independent,
open access, multilingual journal

epaa aape

Arizona State University

Volume 32 Number 3 January 23, 2024 ISSN 1068-2341

# Digital Rights and Responsibility in Education: A Scoping Review[1]

*María-Jesús Gallego-Arrufat*
University of Granada
Spain

*Inmaculada García-Martínez*
University of Granada
Spain

*María-Asunción Romero-López*
University of Granada
Spain

&

*Norma Torres-Hernández*
University of Jaen
Spain

**Citation**: Gallego-Arrufat, M.-J., García-Martínez, I., Romero-López, M.-A, & Torres-Hernández, N. (2024). Digital rights and responsibility in education: A scoping review. *Education Policy Analysis Archives, 32*(3). https://doi.org/10.14507/epaa.32.7899

**Abstract**: Studies on digital rights in education have both gained attention and provided a framework for research, policy and practice in educational research within the field of

[1] European Regional Development Fund's 2014-2020 Operational Program, the Andalusian Government, and Spain's Department of Economic Transformation, Industry, Knowledge and Universities (Project A.SEJ.46.UGR 2020).

Journal website: http://epaa.asu.edu/ojs/
Facebook: /EPAAA
Twitter: @epaa_aape

Manuscript received: 27/11/2022
Revisions received: 20/10/2023
Accepted: 27/11/2023

educational technology. The potential benefits we appreciate in Internet use are inseparable from the maximum risks involved. Faced with this responsibility, individuals demand that their rights and freedoms be guaranteed in the digital environment according to their various roles as students, teachers, families or staff. This scoping review selects and analyses 54 theoretical and empirical studies from the last decade (2013-2023), identifying the main topics investigated as privacy protection in online environments, right to digital security or cybersecurity, and right to digital education. The review underscores the need to guide efforts towards digital education for citizens because the legal regulation of rights and responsibilities is necessary but insufficient. The paper also makes arguments about acceptance, limitations and implications for teacher training.

**Keywords**: digital rights; privacy; Internet use; citizenship education; ethics; educational technology

**Derechos y responsabilidad digitales en la educación: Un estudio de alcance**

**Resumen:** Los estudios sobre los derechos digitales en la educación han llamado la atención y han proporcionado un marco para la investigación, la política y la práctica en la investigación educativa en el campo de la tecnología educativa. Los beneficios potenciales que apreciamos en el uso de Internet son inseparables de los máximos riesgos que conlleva. Ante esta responsabilidad, las personas exigen que se garanticen sus derechos y libertades en el entorno digital, ya sea en su papel de alumnos, profesores, familias o personal. Esta revisión de alcance selecciona y analiza 54 estudios teóricos y empíricos de la última década (2013-2023), identificando como principales temas investigados la protección de la privacidad en entornos en línea, el derecho a la seguridad digital o ciberseguridad y el derecho a la educación digital. La revisión subraya la necesidad de orientar los esfuerzos hacia la educación digital de los ciudadanos porque la regulación legal de derechos y responsabilidades es necesaria, pero insuficiente. El documento también presenta argumentos sobre la aceptación, las limitaciones y las implicaciones para la formación del profesorado.

**Palabras-clave:** derechos digitales; privacidad; uso de Internet; educación para la ciudadanía; ética; tecnología educativa

**Direitos e responsabilidade digitais na educação: Um estudo de escopo**

**Resumo:** Os estudos sobre os direitos digitais na educação ganharam atenção e forneceram um quadro para a investigação, a política e a prática na investigação educacional no domínio da tecnologia educativa. Os benefícios potenciais que apreciamos na utilização da Internet são inseparáveis dos riscos máximos envolvidos. Face a esta responsabilidade, os indivíduos exigem que os seus direitos e liberdades sejam garantidos no ambiente digital, quer no seu papel de estudantes, professores, famílias ou funcionários. Esta revisão de âmbito selecciona e analisa 54 estudos teóricos e empíricos da última década (2013-2023), identificando os principais tópicos investigados como a proteção da privacidade em ambientes em linha, o direito à segurança digital ou cibersegurança e o direito à educação digital. A análise sublinha a necessidade de orientar os esforços para a educação digital dos cidadãos, uma vez que a regulamentação jurídica dos direitos e responsabilidades é necessária mas insuficiente. O documento apresenta também argumentos sobre a aceitação, as limitações e as implicações para a formação de professores.

**Palavras-chave:** direitos digitais; privacidade; utilização da Internet; educação para a cidadania; ética; tecnologia educativa

# Digital Rights and Responsibility in Education: A Scoping Review

Whether the Internet supports and safeguards human rights depends not only on governments, companies and institutions, but on all citizens. Digital education of citizens plays an essential role in digital rights and responsibility (DD&R). Protecting people's individual and collective rights and promoting responsible Internet use is key to the United Nations' (UN) 2030 Agenda. The universal objective is to ensure that fundamental rights and freedoms are upheld while citizens take responsibility for their own safe and responsible Internet use. In a context of globalisation and digital transformation, digital rights emerge as an extension of the rights included in the Universal Declaration of Human Rights, as the application of these rights to the online world. In some countries, public or private organisations have undertaken initiatives to create a Charter of Digital Rights, as well as global communities such as Ranking Digital Rights. Some form of regulation and/or legislation to protect personal data or the right to access information on the Internet exists in more than 120 countries. Supranational organisations such as the European Union (EU) have agreed on a common framework regarding the right to personal data protection—the General Data Protection Regulation [GDPR] (2016). The GDPR establishes common guidelines for data protection and defence of digital rights in EU member states (European Union, 2016).

DD&R must be addressed because, while the Internet pervades almost all aspects of our lives, its threat to privacy can undermine the benefits of its use (O'Neil, 2001). Privacy has become an essential social, political, technological and academic issue, and is postulated as an emerging new right. In educational institutions specifically, tensions with privacy laws and practices are emerging. A growing number of security incidents in higher education institutions highlight the importance of confidentiality, integrity and availability of information in universities (Bongiovanni, 2019). Online privacy is an increasingly important issue, but users/consumers have different levels of concern (Sheehan, 2002). In education, new ethical dilemmas arise with the use of social networks for academic purposes, learning analytics (LA), digital security, artificial intelligence (AI) and big data. The ethical considerations and moral tensions academics, researchers and administrators experience in LA are topics of specific focus (Lawson et al., 2016). Privacy and data ownership are increasingly important to everyone, and privacy and ethics concerns are seen as an emerging field of research (Siemens, 2013). The topic is both timely and necessary, even requiring an idea of data justice—the fairness of how people are made visible, represented and treated as a result of their digital data production—to determine ethical pathways through a world of data (Taylor, 2017). There is thus a need for an overview that explores digital rights studies, such as Internet access, expression freedom and the right to privacy (Daskal, 2018), as well as digital education for safe, responsible and ethical Internet use. Such a study must highlight promotion of social responsibility by engaging institutions, families and citizens.

## Background

### Digital Rights

The concept of digital rights involves rights that assist citizens in accessing, using, creating and publishing in digital media, as well as accessing and using computers, other electronic devices and communications networks. The three terms digital rights, digital citizenship and digital literacy capture epistemological and ontological frames that theorise and enact (in both policy and everyday social interactions) how individuals learn to live in digitally mediated societies (Pangrazio & Selwyn, 2019). The European Declaration on Digital Rights and Principles for the Digital Decade (European Commission, 2022) provides a framework for citizens and guidance for businesses and policy makers to put people at the heart of the digital transformation. It advocates solidarity, inclusion and defence of freedom of choice as core principles. The principles can be grouped into five categories: freedom rights (data protection, digital identity), equality rights (access gaps, accessibility), participation and shaping of public space (citizen participation through digital tools, freedom of expression), work and business environment rights (digital disconnection, corporate digital controls) and digital rights in specific environments. The latter includes rights involving technological development and sustainable digital environments, freedom of creation and access to culture or protection against inequality that may result from AI or data mining, among other issues (Government of Spain, 2021). LA use is considered especially complex and multifaceted in education. It raises ethical and legal challenges due to competing stakeholder views and implementation decisions (West et al., 2020). These debates reflect concerns expressed in studies on LA use's impact on student privacy and autonomy (Buckingham & Ferguson, 2012; Scott & Nichols, 2017; Slade & Prinsloo, 2013). In any case, there is a need for certain non-technical solutions to guarantee the ethical and responsible use of people's digital rights. These solutions are focused on providing information and education regarding the safe and responsible use of all the tools that are available to citizens.

## Responsibility in Online Environments

In this context, safe, responsible, ethical use of technology is essential; people must be educated in the development of digital responsibility. Technical issues coexist with issues that concern the citizen user. Development of technical solutions (procedures and good practices to identify risks, mechanisms to prevent protection of privacy and personal data, security of networks and information systems) must clearly be complemented with non-technical solutions that focus on informing and educating people in safe, responsible use of these tools. They form part of digital competence, understood as "the understanding and critical, responsible and efficient use of media, digital tools and digital resources to solve a case or a task and, in a more general meaning, to be a responsible citizen" (Hatlevik & Tømte, 2014, p. 719). For Choi et al. (2018), one important goal of education is to develop responsible, digitally active citizens who can make informed decisions in a web-based, connected society. The solution to the ethical and social problems of technology use is educating people in the ethical and socially responsible ways of using technology—basically in taking responsibility for the consequences of their actions and behaving appropriately.

## Information Literacy and Digital Competence in Security for Online Risks

We must ask whether young people are digitally competent and use information and communication technologies (ICT) responsibly (Frau-Meigs et al., 2017); and whether future teachers are prepared to meet and overcome the challenges of increasing digitisation (Gudmundsdottir et al., 2020). Technologies have become an important component of initial teacher education and continuing professional development for in-service teachers. Having professional digital competence is becoming an essential part of teacher education, a field in which responsible use of ICT is a key issue (Gudmundsdottir et al., 2020). Teachers' digital competence must be enhanced during their initial training to prepare them to overcome the online risks they will encounter in their studies (Gudmundsdottir & Hatlevik, 2018; Instefjord & Munthe, 2017). Further, as future teachers, they will have to prepare their students for development of digital competence for online risks (Choi et al., 2018). In EdTech in particular, the issue of big data raises ethical challenges about the privacy and security of student data, the role of traditional educational actors-teachers, parents, school administrators, school boards, state departments of education, and national departments of education, as well as the role of new educational actors, particularly online educational technology and software companies (Regan & Jesse, 2019). Personalized learning involves the risk of programs that track and sort learners, potentially leading to discriminatory treatment (Regan & Jesse, 2019) by associating certain outcomes with certain characteristics (e.g., offering a specific race-based content), as well as incorporating discriminatory datafication processes (e.g., only two gender choices) (Jones & Regner, 2016). Such practices create so-called "filter bubbles" (Pariser, 2011), also known as "echo chambers" (Turow, 2013). To decrease the effect of online risk, research recommends raising privacy awareness through cooperation with social media by displaying tips or warnings (Wisniewski et al., 2016; Martin et al., 2018; Wisniewski et al., 2017; Chugh & Ruhi, 2018; Haffner et al., 2018), but without identifying exactly the causes of poor privacy management with generic advice (Chen & Wen, 2019). The opportunities the Internet offers in the information age have been accompanied by new security requirements, which manifest themselves in different ways: a constantly evolving landscape of IT best practices; new regulatory requirements for data protection (e.g., the recent General Data Protection Regulation in Europe or the Data Breach Notification scheme in Australia); and a scenario of new ethical issues that must be addressed in digital education (Bongiovanni, 2019).

## Previous Systematic Reviews

We currently lack comprehensive studies on this subject. No systematic reviews have been performed of DD&R in education, although some related reviews can be found within systematic reviews of big data, digital gaps, or digital competence in security, among other areas. Favaretto et al. (2019) on uses of big data and data mining thus aim to understand the causes and consequences of discrimination in data mining, identify barriers to fair data mining, and explore possible solutions to this problem. Scheerder et al. (2017) conduct a systematic review of the determinants of digital gaps, showing that the third-level digital gap is underexposed. Their main results are that research focuses primarily on Internet use, and that digital gap research is largely limited to sociodemographic and socioeconomic factors. The review by Spante et al. (2018) attempts to establish an understanding of digital literacy and digital competence. The authors identify a variety of definitions in higher education research and find that this research varies depending on whether the concepts are defined by policy, by research, or by both; and whether studies address technical skills or social practices. They recommend research based on critical perspectives (that is, taking development of definitions of these concepts seriously). Such research is needed to avoid using merely the colloquial meaning of these concepts, which can lead to incompatible cross-references, and to engage in critical research on the legitimacy of policy in higher education research. Recently Torres-Hernández and Gallego-Arrufat (2022) conducted a systematic review on preservice teachers' digital competence in security to obtain indicators to assess the area of security of teachers' digital competence. Other systematic reviews conclude that little evidence exists on whether LA improves learning outcomes or is related to positive effects on student achievement (Viberg et al., 2018).

Conducting the first review of its kind, Bongiovanni (2019) concludes that information security management in Higher Education (HE) is a very under-researched topic. The studies reviewed focus primarily on organisational and management issues related to information security. Only three studies focus primarily on information security culture and awareness (Parsons et al., 2017; Singh et al., 2013; Siponen et al., 2014). International standards and shared best practices are another emerging topic. These studies examine information security based on agreed-upon practices and standards to advance more unexplored topics, such as human factors, perceptions and behaviours. The essay concludes that significant gaps exist in the literature on information security management in HE. Future research notes the need to attend to the quality of the studies reviewed and recommends further analysis in four areas: information security culture, understanding the different degrees of awareness of students, researchers, visitors, and staff members, and assessing and improving information security training; comparative studies on information security management in HE and other sectors traditionally considered best practices (e.g., banking or aviation); comparative studies across universities to facilitate dissemination of exemplary cases; and the economics of information security management to support senior management in budgetary decisions and resource allocation. Another review of EdTech articles from 2013 to 2017 in faculty-oriented trade and professional publications reveals that discussion of ethical issues highlights privacy issues framed almost exclusively in terms of protecting student information from inappropriate access or secondary use and discussed in terms of compliance with standard fair information practices (Regan & Jesse, 2019). Due to the lack of scoping reviews on this topic, it has been decided to conduct this type of review, as the purpose of a scoping review is to identify gaps in knowledge, define a literature frame, clarify concepts, investigate research patterns, or inform a systematic review (Munn et al., 2018).

### Purpose

There are new ethical dilemmas in education regarding the use of online tools and programmes for academic purposes that call for research that examines the presence of digital rights and the promotion of responsibility for safe use of the internet. Based on the foregoing, this study aims to explore international studies on the presence in the educational field of digital rights and responsibility on Internet. In this respect, this scoping review seeks to answer the general question: What studies have been conducted in the field of education that address issues of digital rights and responsibility on the internet? More specifically, the following specific objectives are to be achieved:

1. To explore the topics and research designs that address DD&R studies in the field of education.
2. To find out the population sectors involved in the studies and the attitudes of the participants towards DD&R.
3. To examine the issues related to the acceptance and limitations of the implementation of DD&R in education and its projection in teacher education.
4. To understand the implications for the improvement of digital education.

## Method

This study adheres to the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analysis) guidelines and recommendations by following the PRISMA-ScR extension for scoping reviews (Tricco et al., 2018).

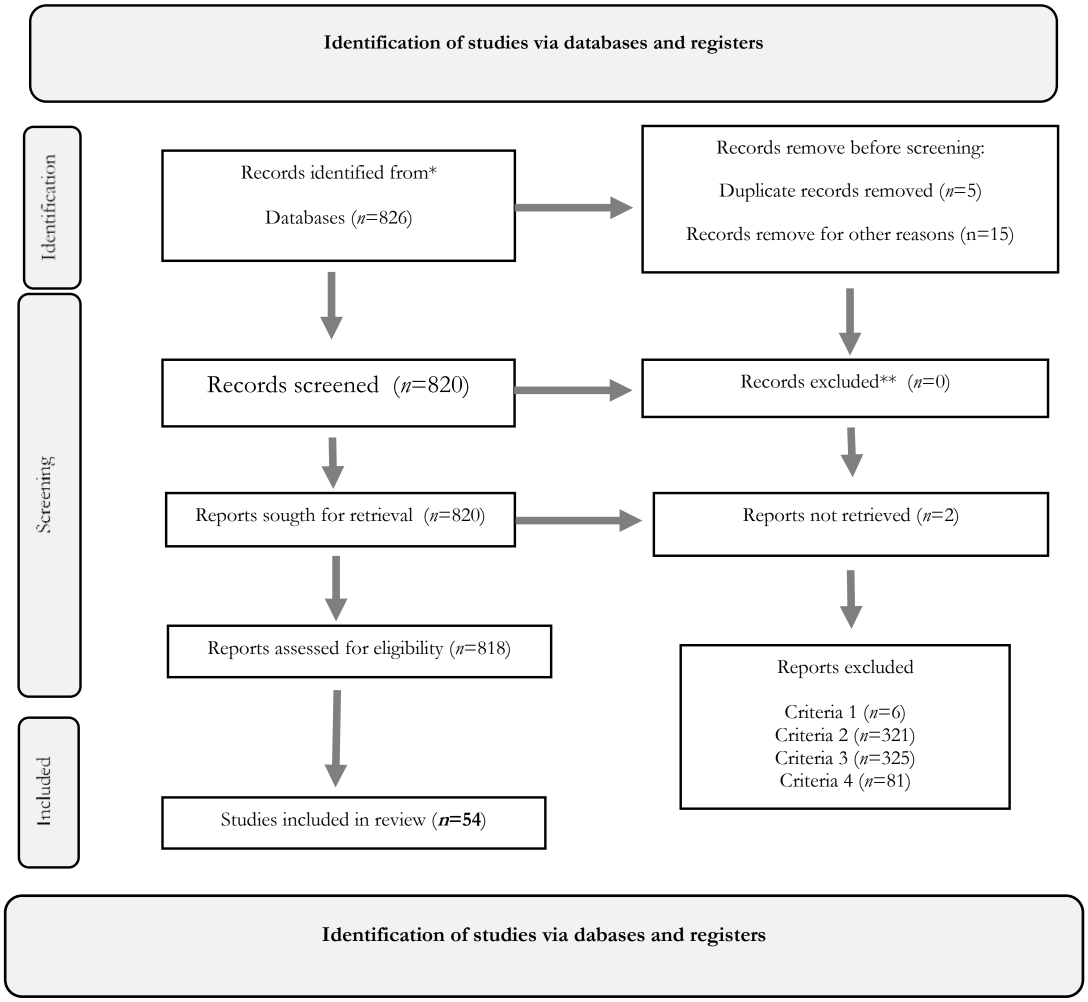
### Search Strategy

The search was performed in the Web of Science Core Collection - Social Science Citation Index (SSCI) database by introducing the following keywords in the following search equation: ((TS=("Digital Rights")) OR TS=((Responsib* AND "Internet use"))) OR TS=("Information security" OR "Data security" OR Privacy OR "Data protection" OR Confidentiality OR "Personnel data" OR "Digital well-being") AND TS=(Education OR ("Digital Citizenship" OR "Citizenship Education")). The search resulted in a total of 826 records.

### Selection Process

The papers found were analysed by the search via identification, screening and eligibility processes, using the following inclusion criteria: a) only articles; b) whose main purpose was to analyse digital rights and/or responsibility in Internet use; c) with an educational approach; d) published from 2013 to 2023; and e) any geographical area, as we aimed to collect as many studies as possible in order to explore the topic in depth. The only exclusion criteria considered thus belonged to Life Science Biomedics. The resulting final sample of items in the review consisted of 54 articles (Figure 1).

**Figure 1**
*Flowchart*


Identification of studies via databases and registers
Identification
Screening
Included
Records identified from*
Databases (n=826)
Records remove before screening:
Duplicate records removed (n=5)
Records remove for other reasons (n=15)
Records screened (n=820)
Records excluded** (n=0)
Reports sougth for retrieval (n=820)
Reports not retrieved (n=2)
Reports assessed for eligibility (n=818)
Reports excluded
Criteria 1 (n=6)
Criteria 2 (n=321)
Criteria 3 (n=325)
Criteria 4 (n=81)
Studies included in review (n=54)
Identification of studies via dabases and registers

The search process was sequenced in two phases—the initial preselection phase, in which the inclusion criteria were applied by reading the title and abstract; and a second more comprehensive phase, in which full manuscripts were read. The first screening of title and abstract yielded 86 articles, eliminating *n*=6 due to criterion 1, *n*=321 due to criterion 2, *n*=325 due to criterion 3, and *n*=81 due to criterion 4. In the second phase, the sample consisted of 54 articles, but 32 were eliminated due to criteria 2 (*n*=18) and 3 (*n*=14), respectively. The four authors participated actively in both phases of the review. The process involved preparing a document in the form of a template, identifying the most relevant characteristics of each item in order to determine its suitability. Once this part was completed, suitability of the items included was compared until 100% agreement was reached among all the researchers.

### Data Extraction

Table 1 (See Appendix) shows the most relevant identifying data in the articles that compose this review sample. These data are: a) author and year), b) purpose of the study, c) population, d) sample, e) instruments and f) DD&R indicators.

## Results and Discussion

This scoping review aims to explore existing international studies systematically in terms of educational approach to DD&R in Internet use. The topic generated the analysis of 54 articles. The four research questions are answered below.

### 1. To explore the topics and research designs that address DD&R studies in the field of education

The thematic analysis of the studies included in this review showed that there are four main areas of interest in this field: privacy, informed consent, personal data protection and ownership. This was followed by issues related to data validity and integrity. Then governance and accountability, and finally the importance of training, awareness and education. For each theme, the authors address in different ways the ethical challenges that were highlighted, albeit with relatively different approaches.

In relation to the research design, due to this being a relatively emerging topic, half of the studies selected are theoretical (*n*=27), and most of these adopt a framework on issues considered in education to preserve the digital rights of citizens on Internet.

Some of these studies addressed issues related to digital rights and guarantees from different theories, conceptual models, paradigms and approaches: the holistic information security management approach (Bongiovanni, 2020); the problem-based approach to analysing privacy (Brinkman, 2013); the cultural information and media literacy approach (Daskal, 2017); distributive justice theory, liberalism and individualism, privacy theory, learning analytics, creeping surveillance, utilitarianism, relativism, care ethics, structural justice, rational pedagogy, semiotic materialism, discrimination theory, governance theory and connectionist learning, the balancing test, ethics of care (Hakimi et al., 2021); Foucault's discourse theory and governmentality (Hope 2015); secular approach to privacy, machine learning theory and AIDA's ethical approach to education (Jones, 2019b); risk and security paradigm (Livingstone & Third, 2017); data monitoring ecosystem (Marachi & Quill, 2020); Taylor's data justice framework theories (Brown & Klein, 2020); Kant's notion of goodwill (Marshall, 2014); new literacy studies approach (Pangrazio & Selwyn, 2019); personalised learning theory (Regan & Jesse, 2019); digital sociology (Selwyn (2015), and a structural justice approach, which possesses a socio-critical perspective (West et al., 2020).

In relation to principles, Vanacker (2011) considers that fair information practices could help alleviate some of the broader concerns that exist in reference to the digitisation of student work; educators must respect students' right to privacy when implementing authorship and originality control systems and Solove's taxonomy (Brinkman, 2013); principles related to the cultural information framework, personal activism and branded digital rights activism (Daskal, 2017); principles of individual control, transparency, respect for context, security, access and accuracy, selective collection and accountability (Jones, 2019a).

Similarly, the empirical studies most commonly used the questionnaire as the instrument most used or as the only measure (n=16), followed by the interview (*n*=5). Two studies used the questionnaire and interview together, one of these combining interviews with the focus group and another in which the questionnaire is a hybrid, including both quantitative and qualitative parts.

Similarly, only three studies were conducted with a quasi-experimental pre-post design, a fact that shows the need for more research of this nature in this area. A similar upward trend is observed in the period 2011–2022 in the number of publications by publication year. Specifically, 2019 showed the highest concentration in the number of articles (n=15), followed by 2020 (*n*=12) and 2021 (*n*=6). The slightly lower number in 2020 and 2021, as well as the absence of studies to date in 2022, is not an indicator of the absence of manuscripts on DD&R. The data imply that studies that address the topic exist but that this is not their main objective. For this reason, we did not include them.

### 2. To find out the population sectors involved in the studies and the attitudes of the participants towards DD&R

The results of this review found eighteen research studies in higher education, ten of which address the issue from the perspective of university students, focusing both on the security and privacy of device use (Abraham & Chengalur-Smith, 2019; Ifenthaler & Schumacher, 2016; Jones, 2020b; Lawson et al., 2016; Walton et al., 2015; Whitelock-Wainwright et al., 2019), and digital rights (Chen & Wen, 2019; Dennen & Burner, 2017; Gudiño et al., 2021; Kim, 2021). Four studies approach the topic from the perspective of university student teachers, i.e. future teachers, and address the use of technologies and their risks (Gallego-Arrufat et al., 2019; Gudmundsdottir et al., 2020), digital identity (Okada et al., 2018) and digital rights (Marín et al., 2020). Two investigations address the topic from educators and draw on the theme of security, privacy and protection issues in virtual environments (Farahmand et al., 2013), as well as on copyright (Okada et al., 2019). Only one study investigates from the perspective of student career counsellors, focusing on cybersecurity and professional ethics in data use (Jones, 2019b). Finally, one research focuses on university employees, focusing on the right to privacy protection in digital environments (Rajab & Eydgahi, 2019) and emphasising the security and integrity of the information they handle.

As to target population attitude, the review finds that many students assume the risks associated with online environments and processing of their personal data on the Internet, while recognising that they could be more cautious about their privacy in different environments. Most papers argue that digital literacy should take a theoretical approach, indicating the need to teach both students and the general population to reduce these risks as much as possible and to increase these groups' awareness of these risks so that they comprehend their responsibility. One study also analyses the implications of student data analytics in educational contexts for students' privacy and digital responsibilities from a policy perspective.

The studies developed in higher education point to the need for digital training and education for learning/teaching in the educational context. They stress the ethical implications and the need to guarantee a safe online educational environment, placing special emphasis on digital education, privacy and security or cybersecurity, while recommending investment in training applied to security for the university community in general.

As for research at other educational levels, there are two studies; both deal with security and digital rights from the perspective of teachers, one focusing on the training of students in early childhood and primary education for digital citizenship (Lauricella et al., 2020); and the other on the role of schools in protecting the personal information of primary and secondary school students (Lupton, 2021).

Focusing on the general population, there are some research studies on children and adults, families and users of the Internet or LinkedIn. In terms of the child and adult population, only one of the studies addresses, from the perspective of parents, teachers and students, perceptions of the risks and benefits of using social networks, both at home and at school (Hayes et al., 2021). For families, one study found deals with privacy, safety and everyday use of digital technology (Kumar et al., 2020).

Research focusing on Internet users focuses on e-privacy management and its relationship with educational level (Maineri et al., 2021) and privacy and digital literacy (Park, 2011). Another focuses on LinkedIn Groups, with a focus on the right to privacy protection in digital environments (Tamjidyamcholo et al., 2014).

### 3. To examine the issues related to the acceptance and limitations of the implementation of DD&R in education and its projection in teacher education

The studies included in this review report heterogeneous data on acceptance of responsibilities for management of personal data and use of various technological platforms where flows of personal information exchange occur. Although the studies analyse acceptance from different perspectives, only two articles included include acceptance by incorporating an instrument to examine the notion and relate it to use of LA and electronic authentication and these studies focus on university students (Ifenthaler & Schumacher, 2016; Okada et al., 2019; Okada et al., 2018). In these cases, students show some resistance to exchanging their data and interacting freely in virtual learning environments. Other participants, in contrast, express a high degree of agreement with acceptance to process their data, asserting that they can manage them properly. This finding highlights a possible direct and positive relationship between digital competence (technological training/literacy) and levels of user acceptance.

Teacher training may represent one line of measures to ensure that students are equipped with the necessary knowledge and skills to perceive online risks, determine how to manage them appropriately and thus be able to reduce resistance to them. Teacher training should be combined with greater awareness and assumption of responsibility for the risks involved in the different resources and platforms used to design and develop instructional processes. Differences have been found in attitude, depending on the nature of the learning management system and transparency of the purposes for which the information collected will be used. Another study indicates that students' attitudinal change and the effectiveness of LA must be meshed with the number of information requirements and the willingness of students to disclose too much information (Ifenthaler & Schumacher, 2016).

In the implementation of DD&R, ethical issues were identified as doubts about established guidelines on fair information practices and data protection in the use of anti-plagiarism tools (Vanacker, 2011); lack of transparency of data ownership issues in e-learning and conflicts about what is personal data versus non-personal data while using free and commercial tools (Ashman et al., 2014); the existence of vulnerabilities in Blockchain technology on security and privacy issues for the exercise of the right to anonymity in virtual learning environments and the strong fragility in privacy, confidentiality and security during the treatment of privacy, confidentiality and security issues in e-learning); existence of vulnerabilities in Blockchain technology on security and privacy issues for the exercise of the right to anonymity in virtual learning environments and the strong fragility in privacy, confidentiality and security during the treatment of educational data in Learning Analytics processes and within EVAs, (Amo et al., 2020); lack of information to students by teachers when using anti-plagiarism tools (Brinkman, 2013); the use of digital tracking data and the concomitant renegotiation of legal, accountability and governance structures in education (Hakimi et al., 2021); the lack of student input into learning analytics (LA) in education raises serious ethical concerns and suggests the need for several actions, such as student engagement around what is being measured, who has access to the data and how the data is being used (West et al., 2020). In turn, the results of this review show that there is a positive and strong relationship between knowledge sharing behaviour and expectations of reduced information security risks (Tamjidyamcholo et al., 2014).

Finally, some of the main issues around digital rights in education in these studies relate to lack of awareness and lack of effective communication and consultation with students and staff as key stakeholders. There is also a lack of knowledge about the use of student data and in particular about the use of student data for learning in higher education (Braunack-Mayer et al., 2020); low involvement of young people in technology design and decisions about privacy and data protection (Zamam, 2020); low awareness of internet rights (Daskal, 2017) as education professionals lack knowledge on the subject (Deane et al., 2015); and the prevalence of little research related to information security in higher education (Bongiovanni, 2020).

### 4. To understand the implications for the improvement of digital education

The 54 studies included in this review provide insight into a wide variety of issues related to an approach that enhances digital education, both in online environments and in managing learning systems. It is important to note that most of the educational implications arise from the processing of data, whether from students, workers or the general population. This calls for the need to improve awareness of the potential ethical issues associated with the use of big data and predictive data analytics in the tertiary education sector and the realisation of data governance arrangements. This includes enabling systems and organisational structures and clear policy guidance for faculty and staff (Braunack-Mayer et al., 2020); educating the public about their rights in the digital age (Daskal, 2018); better training for education professionals on data interpretation (Hakimi et al., 2021); institutions should strive to educate students about the motivations driving educational data mining practices and demonstrate how such practices align with higher education standards, values and expectations (Jones, 2019b).

Thus, in relation to the right to privacy protection in online environments are the need to ensure regulatory frameworks that guarantee privacy in processing of student data (Braunack-Mayer et al., 2020; Kitto & Knight, 2019; Marshall, 2014) by pointing to the transitory nature of students' identity throughout their educational process (Slade & Prinsloo, 2013). This goal requires greater transparency in management, processing and storage of the students' data and involvement of students at all times, both in information shared and in using this information (Jones, Asher et al., 2020). Informed consent models must indicate the type of information that can be collected, while offering students the possibility of selecting the type of information they provide to educational institutions (Jones, 2019a; Selwyn, 2015; West et al., 2020). Research provides a wake-up call on the dangers of managerialism and control of LA, as well as cultural patterns of surveillance and control that may enhance inequalities among students by focusing exclusively on data (Lawson et al., 2016). In this vein, it is necessary to establish frameworks that advocate for secure information management in HE institutions (Bongiovanni, 2019) to establish collective awareness of the importance of security through increased training, sensitivity and transparency (Jones, 2019b). A relationship has also been found between data sharing behaviour, the expectation of information security risk reduction (Ashman et al., 2014; Tamjidyamcholo et al., 2014), and perceived usefulness (Kim, 2021). This finding evidences the need to create literate users knowledgeable of the inherent consequences of information sharing to facilitate safe exchanges and navigation in online environments. Studies also stress that the related concern of developing personalised learning itineraries based on analytics and certain tools (Brinkman, 2013) may undermine the students' digital rights. Greater transparency is needed in the process, adding the component of literacy to optimise consequences (Ashman et al., 2014), fuller definition and stricter legislative enforcement of data management (Jones & Regner, 2016). The study by Amo et al. (2020) supports using Blockchain to reduce many problems associated with security and risks in virtual learning environments.

Other research has examined this digital right from non-student perspectives. Analysing university employees, Rajab and Eydgahi (2019) found that professionals' motivation towards data protection, coupled with training in digital security, contributed to a more secure processing of LA. Analysis of faculty yields heterogeneous results on their perceptions of risk and security (Farahmand et al., 2013), depending on their familiarity, use and security training.

All papers subscribing to the right of protection in online environments underscore the benefits of learning management systems and big data. They also call, however, not only to strengthen security measures and consider ethical issues in the design, planning and execution of instructional processes as places to share knowledge and data but also the infrastructure and management of the platforms in which they take place.

Some studies identify students' resistance to sharing information (Ifenthaler & Schumacher, 2016). Acceptance of use of their data is closely linked to their perception of its usefulness. Acceptance will evolve if the information is used to personalise their learning process through self-assessments, scaffolding and suggested content to foster their self-regulation. Another important issue in the analysis of digital security and public education is the need to promote personal data literacy, seeking efforts to interpret the data based on the context in which it is generated. Pangrazio and Selwyn (2019) suggest that literacy should focus on development and acquisition of meta-knowledge strategies, technical skills, and understanding of how personal data operate within analytics; and that the complexity of literacy demands the collective attention and support of others.

Social networks and students' digital identity are another issue addressed by the right to cybersecurity (Dennen & Burner, 2017). Walton et al. (2015) conducted an experiment to sensitise medical students and raise their awareness of the importance of properly managing the information they shared on social networks (especially Facebook) and on the Internet in general. Students saw how this information could harm their professional careers. The results obtained revealed that most participants were aware of the risks involved in sharing information publicly, and quite a few participants further restricted the information they shared. The practical implications are the importance of engaging students (and the public) in the risks in online environments and the positive effect of security literacy/training on information sharing practices.

On the right to digital education, all studies stress the importance of initiating digital literacy processes among various stakeholders: among students (Abraham & Chengalur-Smith, 2019; Chen & Wen, 2019; Kumar et al., 2020; Livingstone & Third, 2017), pre-service (Gallego-Arrufat et al., 2019; Gudmundsdottir et al., 2020; Marín et al., 2021) and in-service (Gudmundsdottir et al., 2020; Jones & VansCoy, 2019; Lauricella et al., 2020; Rennie et al., 2019) teachers, students and families together (Hayes et al., 2021), and the general population (Daskal, 2018; Park, 2011; Maineri et al., 2021). The goal is to develop skills to use and manage technological tools, platforms and shared information, while teaching the risks, rights and responsibilities of which users should be aware for effective web browsing.

Regarding the GDPR law, Zaman's study (2020) advocates involving young people in designing instructional processes in online environments from a critical perspective. Among the main challenges identified are viewing young people as consumers of digital products rather than as citizens who must be literate to exercise all their rights; and designing real active participation situations, in which young people have space and voice to choose before implementing the learning experience. Opportunities also involve empowering students to decide about their privacy and determine what they are willing to share, with full awareness of their purpose.

Although the analysis of the topic by geographical area was not part of the objectives of this review, the findings obtained have shown a direct relationship between digital skills and Internet use, concluding that the educational gap in e-privacy management is reduced in the most digitised countries (Maineri et al., 2021; Park, 2011). A particular emphasis is placed on digital education, privacy and security or cybersecurity.

## Limitations and Future Research

One limitation derives from using only one language and one database; greater diversity would provide a more globalised, less institution-centred view of HE. Philosopher Hannah Arendt´s famous phrase about, *the right to have rights* could be used in the context of studies on the rights to equality and non-discrimination or universal accessibility obligations. Digital rights based on gender, rural context, vulnerable area, or population at risk of exclusion should be the subject of prospective studies, using low and lower-middle income countries as inclusion criteria.

## Conclusion

This paper has documented ongoing growth in research on the topic of DD&R. Most papers were published in 2019 or later, demonstrating growing interest and the need to increase research efforts in this area. The most relevant studies of DD&R in education and of the literacy/training needed to ensure compliance relate to topics of interest for all education sectors: big data, data mining useful for personalised learning and LA in higher education; ethical responsibility of education professionals to preserve students' privacy, including that of teachers, students and staff; social media use combined with learning management systems; topics of interest to families, students, teachers and staff at all stages of education; the promotion of digital security competence and the development of privacy policies in education. It is important to note that regulation and legislation around the use and abuse of personal information is extremely diverse. Although some similarities or supra-national proposals exist, such as the European GDPR, the North American, Asian, Australian and European contexts have little in common. Analysis of studies on DD&R in education thus encounters dilemmas and challenges. Despite globalisation and the worldwide digital transformation, regulations for protection of individuals in processing personal data and for free movement of such data are published and applied only after the population has access to applications from technology, online software, or telecommunications companies to carry out online communications for educational purposes. In any case, the importance of empowering and including digital education for learning in the educational context has been highlighted, stressing the ethical implications and the need to ensure a safe online educational environment.

## References

*Abraham, S., & Chengalur-Smith, I. (2019). Evaluating the effectiveness of learner controlled information security training. *Computers & Security*, *87*, 101586. https://doi.org/10.1016/j.cose.2019.101586

*Amo, D., Alier, M., García, F. J., Fonseca, D., & Casany, M. J. (2020). Privacy, security and legality in educational solutions based on Blockchain: A systematic literature review. RIED. *Revista Iberoamericana de Educación a Distancia, 23*(2), 213-236. http://dx.doi.org/10.5944/ried.23.2.26388

*Ashman, H., Brailsford, T., Cristea, A. I., Sheng, Q. Z., Stewart, C., Toms, E. G., & Wade, V. (2014). The ethical and social implications of personalization technologies for e-learning. *Information & Management, 51*(6), 819-832. https://doi.org/10.1016/j.im.2014.04.003

*Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. *Computers & Security*, *86*, 350-357. https://doi.org/10.1016/j.cose.2019.07.003

*Braunack-Mayer, A. J., Street, J. M., Tooher, R., Feng, X., & Scharling-Gamba, K. (2020). Student and staff perspectives on the use of big data in the tertiary education sector: A scoping review and reflection on the ethical issues. *Review of Educational Research, 90*(6), 788-823. https://doi.org/10.3102/0034654320960213

*Brinkman, B. (2013). An analysis of student privacy rights in the use of plagiarism detection systems. *Science and Engineering Ethics, 19*(3), 1255-1266. https://doi.org/10.1007/s11948-012-9370-y

*Brown, M., & Klein, C. (2020). Whose data? Which rights? Whose power? A policy discourse analysis of student privacy policy documents. *Journal of Higher Education, 91*(7), 1149-1178. https://doi.org/10.1080/00221546.2020.1770045

Buckingham Shum, S., & Ferguson, R. (2012). Social learning analytics. *Journal of Educational Technology & Society, 15*(3), 3-26. https://bit.ly/3hNNn9J

*Chen, Y. K., & Wen, C. R. (2019). Taiwanese university students' smartphone use and the privacy paradox. *Comunicar, 27*(60), 61-69. http://dx.doi.org/10.3916/C60-2019-06

Choi, M., Cristol, D., & Gimbert, B. (2018). Teachers as digital citizens: The influence of individual backgrounds, internet use and psychological characteristics on teachers' levels of digital citizenship. *Computers & Education*, *121*, 143-161. https://doi.org/10.1016/j.compedu.2018.03.005

Chugh, R., & Ruhi, U. (2018). Social media in higher education: A literature review of Facebook. *Education and Information Technologies, 23*(2), 605-616. https://doi.org/10.1007/s10639-017-9621-2

*Daskal, E. (2018). Let's be careful out there…: How digital rights advocates educate citizens in the digital age. *Information, Communication & Society, 21*(2), 241-256. https://doi.org/10.1080/1369118X.2016.1271903

*Deane, F. P., Gonsalvez, C., Blackman, R., Saffioti, D., & Andresen, R. (2015). Issues in the development of e-supervision in professional psychology: A review. *Australian Psychologist, 50*(3), 241-247. https://doi.org/10.1111/ap.12107

*Dennen, V. P., & Burner, K. J. (2017). Identity, context collapse, and Facebook use in higher education: Putting presence and privacy at odds. *Distance Education, 38*(2), 173-192. https://doi.org/10.1080/01587919.2017.1322453

European Commission. (2022). *European Declaration on Digital Rights and Principles for the Digital Decade.* https://bit.ly/3vXA52q

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

*Farahmand, F., Yadav, A., & Spafford, E. H. (2013). Risks and uncertainties in virtual worlds: An educators' perspective. *Journal of Computing in Higher Education, 25*(2), 49-67. https://doi.org/10.1007/s12528-013-9067-5

Favaretto, M., De Clercq, E., & Elger, B. S. (2019). Big Data and discrimination: Perils, promises and solutions. A systematic review. *Journal of Big Data, 6*(12). https://doi.org/10.1186/s40537-019-0177-4

Frau-Meigs, D., O'Neill, B., Soriani, A., & Tomé, V. (2017). *Digital citizenship education: Overview and new perspectives.* Council of Europe. https://bit.ly/34nWHhg

*Gallego-Arrufat, M. J., Torres-Hernández, N., & Pessoa, T. (2019). Competencia de futuros docentes en el área de seguridad digital. *Comunicar, 27*(61), 57-67. https://doi.org/10.3916/C61-2019-05

Government of Spain (2021). *Bill of Digital Rights.* https://bit.ly/3CsgloQ

*Gudiño, S., Jasso, F. D. J., & de La Fuente Alcazar, J. M. (2021). Remote proctored exams: Integrity assurance in online education? *Distance Education, 42*(2), 200-218. https://doi.org/10.1080/01587919.2021.1910495

Gudmundsdottir, G. B., & Hatlevik, O. E. (2018). Newly qualified teachers' professional digital competence: implications for teacher education. *European Journal of Teacher Education, 41*(2), 214-231. https://doi.org/10.1080/02619768.2017.1416085

*Gudmundsdottir, G. B., Hernández Gassó, H., Colomer Rubio, 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

*Gursoy, M. E., Inan, A., Nergiz, M. E., & Saygin, Y. (2016). Privacy-preserving learning analytics: Challenges and techniques. *IEEE Transactions on Learning Technologies, 10*(1), 68-81. https://doi.org/10.1109/TLT.2016.2607747

Haffner, M., Mathews, A. J., Fekete, E., & Finchum, G.A. (2018). Location-based social media behavior and perception: Views of university students. *Geographical Review, 108*(2), 203-224. https://doi.org/10.1111/gere.12250

*Hakimi, L., Eynon, R., & Murphy, V. A. (2021). The ethics of using digital trace data in education: A thematic review of the research landscape. *Review of Educational Research, 91*(5), 671-717. https://doi.org/10.3102/00346543211020116

Hatlevik, O. E., & Tømte, K. (2014). Using multilevel analysis to examine the relationship between upper secondary students Internet safety awareness, social background and academic aspirations. *Future Internet, 6*(4), 717-734. https://doi.org/10.3390/fi6040717

*Hayes, B., James, A., Barn, R., & Watling, D. (2021). "The world we live in now": A qualitative investigation into parents', teachers', and children's perceptions of social networking site use. *British Journal of Educational Psychology, 92*(1), 340-363. https://doi.org/10.1111/bjep.12452

*Hope, A. (2015). Schoolchildren, governmentality and national e-safety policy discourse. *Discourse: Studies in the Cultural Politics of Education, 36*(3), 343-353. https://doi.org/10.1080/01596306.2013.871237

*Ifenthaler, D., & Schumacher, C. (2016). Student perceptions of privacy principles for learning analytics. *Educational Technology Research and Development, 64*(5), 923-938. https://doi.org/10.1007/s11423-016-9477-y

Instefjord, E. J., & Munthe, E. (2017). Educating digitally competent teachers: A study of integration of professional digital competence in teacher education. *Teaching and Teacher Education*, *67*, 37-45. https://doi.org/10.1016/j.tate.2017.05.016

*Jones, K. M. (2019a). 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*(1), 1-22. https://doi.org/10.1186/s41239-019-0155-0

*Jones, K. M. (2019b). Advising the whole student: eAdvising analytics and the contextual suppression of advisor values. *Education and Information Technologies, 24*(1), 437-458. https://doi.org/10.1007/s10639-018-9781-8

*Jones, K. M., Asher, A., Goben, A., Perry, M. R., Salo, D., Briney, K. A., & Robertshaw, M. B. (2020). "We're being tracked at all times": Student perspectives of their privacy in relation to learning analytics in higher education. *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*(5), 1473-1496. https://doi.org/10.1007/s11948-015-9692-7

*Jones, K. M., Rubel, A., & LeClere, E. (2020). A matter of trust: Higher education institutions as information fiduciaries in an age of educational data mining and learning analytics. *Journal of the Association for Information Science and Technology, 71*(10), 1227-1241. https://doi.org/10.1002/asi.24327

*Jones, K. M., & VanScoy, A. (2019). The syllabus as a student privacy document in an age of learning analytics. *Journal of Documentation, 75*(6), 1333-1355. https://doi.org/10.1108/JD-12-2018-0202

*Kim, S. S. (2021). Motivators and concerns for real-time online classes: Focused on the security and privacy issues. *Interactive Learning Environments*, 1-14. https://doi.org/10.1080/10494820.2020.1863232

*Kitto, K., & Knight, S. (2019). Practical ethics for building learning analytics. *British Journal of Educational Technology, 50*(6), 2855-2870. https://doi.org/10.1111/bjet.12868

*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

*Lauricella, A. R., Herdzina, J., & Robb, M. (2020). Early childhood educators' teaching of digital citizenship competencies. *Computers & Education, 158*, 103989. https://doi.org/10.1016/j.compedu.2020.103989

*Lawson, C., Beer, C., Rossi, D., Moore, T., & Fleming, J. (2016). Identification of 'at risk' students using learning analytics: The ethical dilemmas of intervention strategies in a higher education institution. *Educational Technology Research and Development, 64*(5), 957-968. https://doi.org/10.1007/s11423-016-9459-0

*Livingstone, S., & Third, A. (2017). Children and young people's rights in the digital age: An emerging agenda. *New Media & Society, 19*(5), 657-670. https://doi.org/10.1177/1461444816686318

*Lupton, D. (2021). 'Honestly no, I've never looked at it': Teachers' understandings and practices related to students' personal data in digitised health and physical education. *Learning, Media and Technology, 46*(3), 281-293. https://doi.org/10.1080/17439884.2021.1896541

*Lupton, D., & Williamson, B. (2017). The datafied child: The dataveillance of children and implications for their rights. *New Media & Society, 19*(5), 780-794. https://doi.org/10.1177/1461444816686328

*Maineri, A. M., Achterberg, P., & Luijkx, R. (2021). The closing educational gap in e-privacy management in European perspective. *Sociological Research Online*, 13607804211023524. https://doi.org/10.1177/13607804211023524

*Marachi, R., & Quill, L. (2020). The case of Canvas: Longitudinal datafication through learning management systems. *Teaching in Higher Education, 25*(4), 418-434. https://doi.org/10.1080/13562517.2020.1739641

*Marín, V. I., Carpenter, J. P., & Tur, G. (2020). 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

*Marshall, S. (2014). Exploring the ethical implications of MOOCs. *Distance Education, 35*(2), 250-262. https://doi.org/10.1080/01587919.2014.917706

Martin, F., Wang, C., Petty, T., Wang, W., & Wilkins, P. (2018). Middle School students' social media use. *Journal of Educational Technology & Society, 21*(1), 213-224. https://bit.ly/3hPNJfX

Munn, Z., Peters, M. D., Stern, C., Tufanaru, C., McArthur, A., & Aromataris, E. (2018). Systematic review or scoping review? Guidance for authors when choosing between a systematic or scoping review approach. *BMC Medical Research Methodology*, *18*, 1-7. https://doi.org/10.1186/s12874-018-0611-x

O'Neil, D. (2001). Analysis of Internet users' level of online privacy concerns. *Social Science Computer Review, 19*(1), 17-31. https://doi.org/10.1177/089443930101900103

*Okada, A., Noguera, I., Alexieva, L., Rozeva, A., Kocdar, S., Brouns, F., & Guerrero-Roldán, A. E. (2019). Pedagogical approaches for e-assessment with authentication and authorship verification in higher education. *British Journal of Educational Technology, 50(*6), 3264-3282. https://doi.org/10.1111/bjet.12733

*Okada, A., Whitelock, D., Holmes, W., & Edwards, C. (2018). e-Authentication for online assessment: A mixed-method study. *British Journal of Educational Technology, 50*(2), 861-875. https://doi.org/10.1111/bjet.12608

*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

*Park, Y. J. (2011). Digital literacy and privacy behavior online. *Communication Research, 40*(2), 215-236. https://doi.org/10.1177/0093650211418338

Pariser, E. (2011). *The filter bubble: How the new personalized web is changing what we read and how we think*. Penguin Books.

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, *66*, 40-51. https://doi.org/10.1016/j.cose.2017.01.004

*Rajab, M., & Eydgahi, A. (2019). Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security, 80*, 211-223. https://doi.org/10.1016/j.cose.2018.09.016

*Regan, P. M., & Jesse, J. (2019). Ethical challenges of EdTech, Big Data and personalized learning: Twenty-first century student sorting and tracking. *Ethics and Information Technology, 21*(3), 167-179. https://doi.org/10.1007/s10676-018-9492-2

*Rennie, E., Schmieder, K., Thomas, J., Howard, S. K., Ma, J., & Yang, J. (2019). Privacy and app use in Australian primary schools: Insights into school-based Internet governance. *Media International Australia, 170*(1), 78-89. https://doi.org/10.1177/1329878X19828368

Scheerder, A., Van Deursen, A., & Van Dijk, J. (2017). Determinants of Internet skills, uses and outcomes: A systematic review of the second-and third-level digital divide. *Telematics and Informatics, 34*(8), 1607-1624. https://doi.org/10.1016/j.tele.2017.07.007

Scott, J., & Nichols, T. P. (2017). Learning analytics as assemblage: Criticality and contingency in online education. *Research in Education, 98*(1), 83-105. https://doi.org/10.1177/0034523717723391

*Selwyn, N. (2015). Data entry: Towards the critical study of digital data and education. *Learning, Media and Technology, 40*(1), 64-82.

Sheehan, K. B. (2002). Toward a typology of Internet users and online privacy concerns. *The Information Society, 18*(1), 21-32. https://doi.org/10.1080/01972240252818207

Siemens, G. (2013). Learning analytics: The emergence of a discipline. *American Behavioral Scientist, 57*(10), 1380-1400. https://doi.org/10.1177/0002764213498851

Singh, A. N., Picot, A., Kranz, J., Gupta, M. P., & Ojha, A. (2013). Information security management (ism) practices: Lessons from select cases from India and Germany. *Global Journal of Flexible Systems Management, 14*(4), 225-239. https://doi.org/10.1007/s40171-013-0047-4

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. *Information & Management, 51*(2), 217-224 https://doi.org/10.1016/j.im.2013.08.006.

*Slade, S., & Prinsloo, P. (2013). Learning analytics: Ethical issues and dilemmas. *American Behavioral Scientist, 57*(10), 1509–1528. https://doi.org/10.1177/0002764213479366

Spante, M., Hashemi, S. S., Lundin, M., & Algers, A. (2018). Digital competence and digital literacy in higher education research: Systematic review of concept use. *Cogent Education, 5*(1), 1519143. https://doi.org/10.1080/2331186X.2018.1519143

*Tamjidyamcholo, A., Baba, M. S. B., Shuib, N. L. M., & Rohani, V. A. (2014). Evaluation model for knowledge sharing in information security professional virtual community. *Computers & Security, 43*, 19-34. https://doi.org/10.1016/j.cose.2014.02.010

Taylor, L. (2017). What is data justice? The case for connecting digital rights and freedoms globally. *Big Data & Society, 4*(2). https://doi.org/10.1177/2053951717736335

Torres-Hernández, N., & Gallego-Arrufat, M.J. (2022). Indicators to assess preservice teachers' digital competence in security: A systematic review. *Education and Information Technologies,* 1-20. https://doi.org/10.1007/s10639-022-10978-w

Tricco, A. C., Lillie, E., Zarin, W., O'Brien, K. K., Colquhoun, H., Levac., D, Moher, D., Peters, M. D., Horsley, T., Weeks, L., Hempel, S. et al. (2018). PRISMA extension for scoping reviews (PRISMA-ScR): Checklist and explanation. *Annals of Internal Medicine, 169*(7), 467-473. https://doi.org/10.7326/M18-0850

Turow, J. (2013). *The daily you: How the new advertising industry is defining your identity and your worth.* Yale University Press.

*Vanacker, B. (2011). Returning students' right to access, choice and notice: A proposed code of ethics for instructors using Turnitin. *Ethics and Information Technology, 13*(4), 327-338. https://doi.org/10.1007/s10676-011-9277-3

Viberg, O., Hatakka, M., Bälter, O., & Mavroudia, A. (2018). The current landscape of learning analytics in higher education. *Computers in Human Behavior, 89*, 98110. https://doi.org/10.1016/j.chb.2018.07.027

*Walton, J. M., White, J., & Ross, S. (2015). What's on YOUR Facebook profile? Evaluation of an educational intervention to promote appropriate use of privacy settings by medical students on social networking sites. *Medical Education Online, 20*(1), 28708. https://doi.org/10.3402/meo.v20.28708

*West, D., Luzeckyj, A., Toohey, D., Vanderlelie, J., & Searle, B. (2020). Do academics and university administrators really know better? The ethics of positioning student perspectives in learning analytics. *Australasian Journal of Educational Technology, 36*(2), 60–70. https://doi.org/10.14742/ajet.4653

*Whitelock-Wainwright, A., Gašević, D., Tejeiro, R., Tsai, Y. S., & Bennett, K. (2019). The student expectations of learning analytics questionnaire. *Journal of Computer Assisted Learning, 35*(5), 633-666. https://doi.org/10.1111/jcal.12366

*Williams, M., Nurse, J. R., & Creese, S. (2019). Smartwatch games: Encouraging privacy-protective behaviour in a longitudinal study. *Computers in Human Behavior*, *99*, 38-54. https://doi.org/10.1016/j.chb.2019.04.026

Wisniewski, P. J., Knijnenburg, B. P., & Lipford, H. R. (2017). Making privacy personal: Profiling social network users to inform privacy education and nudging. *International Journal of Human-Computer Studies*, *98*, 95-108. https://doi.org/10.1016/j.ijhcs.2016.09.006

Wisniewski, P. J., Najmul-Islam, A. K., Lipford, H. R., & Wilson, D. C. (2016). Framing and measuring multi-dimensional interpersonal privacy preferences of social networking site users. *Communications of the Association for Information Systems, 38*(10). https://doi.org/10.17705/1cais.03810

*Zaman, B. (2020). Designing technologies with and for youth: Traps of privacy by design. *Media and Communication, 8*(4), 229-238. https://doi.org/10.17645/mac.v8i4.3261

## About the Authors

**María Jesús Gallego-Arrufat**
University of Granada
mgallego@ugr.es
https://orcid.org/0000-0002-2296-5431

Full professor of educational technology, University of Granada, Spain. PhD in education. She is currently leading several projects on digital education, educational actions for digital citizenship, digital rights in education and digital competences of teachers in security. She also publishes on computer-supported learning, communities of inquiry, and blended and virtual learning in higher education.

**Inmaculada García-Martínez**
University of Granada
igmartinez@ugr.es
https://orcid.org/0000-0003-2620-5779

Assistant lecturer at the University of Granada (Spain). She has a PhD in education. She is currently working on professional identity and psychosocial factors related with teachers and professional development. She also investigated abourt educational technology and inclusive education. She has published several scientific articles on pedagogical leadership, school organization, educational technology and emotional intelligence. She is a member of the Ibero-American Network for the Development of Professional Teaching Identity. She has participated in several research projects funded by the Spanish Ministry of Education.

**M$^{a}$. Asunción Romero-López (Corresponding Author)**
University of Granada
romerol@ugr.es
https://orcid.org/0000-0003-1468-7985

Senior lecturer, University of Granada (Spain). PhD in education. Currently works on teachers and professional development, active methodologies and educational technology, has published several scientific articles on pedagogical leadership, educational technology and active methodologies, and has participated in several research projects funded by the Spanish Ministry of Education.

**Norma Torres-Hernández**
University of Jaen
ntorres@ujaen.es
https://orcid.org/0000-0003-4744-0313

Professor at the University of Jaén (Spain). PhD in education. Studies in communication, education and pedagogy. She publishes and researches digital competences in initial teacher training and data protection. Other research interests are: educational technology, curriculum, teacher training and formative assessment. She is currently involved in research projects on safe and responsible use of the Internet and digital rights.

education policy analysis archives

Volume 32 Number 3 January 25, 2024 ISSN 1068-2341

About the Editorial Team: https://epaa.asu.edu/ojs/index.php/epaa/about/editorialTeam

Please send errata notes to Jeanne M. Powers at jeanne.powers@asu.edu

**Join EPAA's Facebook community** at https://www.facebook.com/EPAAAAPE and **Twitter feed** @epaa_aape.

# Appendix

**Table 1**

*Studies Included in the Research*

| Author & year | Aims | Participants | Sample | Instruments | DD&R Indicators |
|---|---|---|---|---|---|
| Abraham & Chengalur-Smith (2019) | To examine the effects of student control on effectiveness of information security training (ISec). | University students | *n*=206; GE:115; GC:91 | Questionnaire | Right to digital education |
| Amo Filvâ et al. (2020) | To explore the importance of personal data protection and security in education through the emerging promises of stakeholders interested in using Blockchain technology. | Theoretical | - | - | Digital security or cybersecurity and other rights |
| Ashman et al. (2014) | To expose the ethical and social implications of personalising e-learning. | Theoretical | - | - | Protection of privacy rights in online environments |
| Bongiovanni (2019) | To examine articles on security breaches experienced by higher education institution in recent years. | Theoretical | - | - | Right to digital security or cybersecurity; Protection of privacy rights in online environments |
| Braunack-Mayer et al. (2020) | To identify articles that describe the views and perspectives of staff and students in the university sector on use of student-generated data through data analytics, including LA. | Theoretical | - | - | Protection of privacy rights in online environments and others. |
| Brinkman (2013) | To focus specifically on plagiarism detection services that make permanent archives of student work, and security and digital rights issues related to use of these tools. | Theoretical | - | - | Authorship rights; Protection of privacy rights in online environments; Responsibility |
| Brown & Klein (2020) | To understand how data privacy policies conceptualise and represent data, privacy, student agency and institutional power | Theoretical | 151 | - | Protection of privacy rights in online environments; Responsibility |
| Chen & Wen (2019) | 1) To understand college students' reasons for smartphone use; 2) To delineate their habitual smartphone use and reaction to social media's targeted advertising; 3) To analyse their privacy management in response to privacy concern over targeting advertising; 4) To identify suitable pedagogies to improve their privacy awareness and management. | University students | 810 | Questionnaire | Right to digital education |
| Daskal (2018) | To determine the strategies that organisations advocating for digital | Theoretical | - | - | Right to digital education |

**Table 1**
*Studies Included in the Research*

| Author & year | Aims | Participants | Sample | Instruments | DD&R Indicators |
|---|---|---|---|---|---|
| | rights employ to involve the public in their cause. | | | | |
| Deane et al. (2015) | To address development of an e-supervision application to overcome these limitations and to examine issues inherent in such development. | Theoretical | - | - | Right to digital security or cybersecurity |
| Dennen & Burner Quemador (2017) | To examine university students' attitudes toward Facebook use, focusing specifically on how they feel about using a social network that encourages performance of personal and social identity to support learning and interaction among classmates and instructors. | University students | 406 | Questionnaires | Digital identity rights; Right to digital security or cybersecurity |
| Farahmand et al. (2013) | To examine how educators perceive risks and uncertainties in virtual worlds; to investigate how educators' level of use of virtual worlds influences their risk perception level. | Educators | 77 | Questionnaire | Protection of privacy rights in online environments |
| Gallego-Arrufat et al. (2019) | 1) To identify preservice teachers' level of digital competence in safety; 2) To describe the competence profile of preservice teachers in different areas of safety (interaction through technologies, sharing of digital information and contents, protection of personal data, protection of health, netiquette, digital identity and cyberbullying on social networks and Internet); 3) To explore differences by sex, gender and age at which one begins using social networks in each of the different areas in order to determine training needs to improve preservice teachers' digital competence in safety; 4) To provide pedagogical activities in safety appropriate to preservice teachers' strengths and weaknesses. | Pre-service teachers | 317 | Questionnaire | Right to digital security or cybersecurity; Right to digital education |
| Gudiño Paredes et al. (2021) | To understand the extent to which remote proctored exams impacted online graduate students' learning process and academic integrity (ethics), as well as the technological factor involved. | University students | 106 | Questionnaire; interviews | Right to digital security or cybersecurity; Responsibility |

**Table 1**

*Studies Included in the Research*

| Author & year | Aims | Participants | Sample | Instruments | DD&R Indicators |
|---|---|---|---|---|---|
| Gudmundsdottir et al. (2020) | To explore how learners' perceptions of trust influence their perceptions of a virtual human's persona and their learning outcomes across three different voice conditions. | Pre-service teachers | 1244 | Questionnaire | Right to digital education; Responsibility |
| Gursoy et al. (2016) | To employ and evaluate methods on learning analytics by approaching the problem from two perspectives: (1) data are anonymised and then shared with a learning analytics expert, and (2) the learning analytics expert is given a privacy-preserving interface that governs her access to the data. | Theoretical | - | - | Right to digital security or cybersecurity; Protection of privacy rights in online environments |
| Hakimi et al. (2021) | Identify and analyse all relevant conceptual and empirical work in the field, with a view to identifying the key ethical issues and their social implications, any responses to such ethical issues (including guidance and frameworks), and areas for further research and policy development. | Theoretical | - | - | Responsibility |
| Hayes et al. (2021) | To explore parents', teachers' and children's perceptions of the risks and benefits of SNS use and how adults mediate this use. | Parents, teachers and students | 13 parents, 14 teachers and 15 students | Interviews | Right to digital education |
| Hope (2015) | To explore how e-safety policy documents serve to constrain the conceptual environment by seeking to determine and limit individuals' thoughts on this matter. | Theoretical | - | - | Right to digital security or cybersecurity |
| Ifenthaler & Schumacher (2016) | To examine student perceptions of privacy principles related to learning analytics. | University students | 330 | Questionnaires | Protection of privacy rights in online environments |
| Jones (2019a) | To provide a conceptual model that demonstrates how learning analytics highlights existing privacy issues and presents new ones related to students' inability to control how institutions use data and information about them. | Theoretical | - | - | Protection of privacy rights in online environments |
| Jones (2019b) 2020 | To provide a platform for advisors to speak about their experiences and concerns related to eAdvising tools with informational and analytic affordances | Professional student advisors | 14 | Interviews | Right to digital security or cybersecurity |

**Table 1**

*Studies Included in the Research*

| Author & year | Aims | Participants | Sample | Instruments | DD&R Indicators |
|---|---|---|---|---|---|
| Jones, Asher et al. (2020) | To explore student perceptions of the capture and use of demographic data, physical and online behavior trails, and other non-academic data. | University students | 120 | Interviews | Protection of privacy rights in online environments |
| Jones & Regner (2016) | To describe and analyse the MOOC phenomenon and the privacy laws and policies that guide and regulate current educational institutions. | Theoretical | - | - | Protection of privacy rights in online environments and others |
| Jones, Rubel et al. (2020) | To understand when it is justifiable to collect, analyse, and use student data in the context of higher education. | Theoretical | - | - | Protection of privacy rights in online environments |
| Jones & VansCoy (2019) | To disclose how instructors discuss student data and information privacy in their curricula. | Theoretical | - | - | Protection of privacy rights in online environments |
| Kim (2021) | To determine whether the security and privacy concerns are the main issues restricting student participation. | University students | 296 | Questionnaire | Protection of privacy rights in online environments |
| Kitto & Knight (2019) | To draw attention to some assumptions that underlie previous work in ethics for LA, framed as three tensions. | Theoretical | - | - | Protection of privacy rights in online environments; Responsibility |
| Kumar et al. (2020) | To analyse children's perspectives on password management in three contexts: family, friendship and education; and to develop a new approach to privacy education based on Nissenbaum's contextual integrity framework. | Families | 70 | Interviews | Right to digital education; Protection of privacy rights in online environments |
| Lauricella et al. (2020) | To document how teaching of digital citizenship skills in primary school varies according to factors such as student demographics and amount of educator experience. | Pre-school and primary school teachers | 1208 | Questionnaire | Right to digital education |
| Lawson et al. (2016) | To expose the ethical dilemmas of using a participation system at CQUniversity (Australia) called Early Alert Student Indicators (EASI) that calculates students' estimated success. | University students | More than 30,000 | - | Protection of privacy rights in online environments |
| Livingstone & Third (2017) | To learn about digital rights and behaviours of children and young people in virtual environments from a theoretical perspective. | Theoretical | - | - | Right to universal access; Right to digital education |

**Table 1**

*Studies Included in the Research*

| Author & year | Aims | Participants | Sample | Instruments | DD&R Indicators |
|---|---|---|---|---|---|
| Lupton (2021) | To understand ways in which digital technologies are used for pedagogical purposes. | Teachers | 5 | Interviews | Responsibility |
| Lupton & Williamson (2017) | To provide an overview of the different forms of datafication and dataveillance of children in the countries of the Global North by presenting theoretical perspectives on the broader implications. | Theoretical | - | - | Right to digital security or cybersecurity; Responsibility |
| Maineri et al. (2021) | To investigate whether and why education affects e-privacy management, and whether education gaps vary according to a country's degree of digitisation. | Internet users | 21,177 | Questionnaire | Right to digital education |
| Marachi & Quill (2020) | To analyse development of Canvas LMS, according to 1) "frictionless" data transitions that bridge K12, higher education and workforce data, 2) integration of third-party applications and interoperability or data-sharing across platforms, 3) privacy and security vulnerabilities and 4) predictive analytics and dataveillance. | Theoretical | - | - | Protection of privacy rights in online environments; Right to digital security or cybersecurity |
| Marín et al. (2020) | To address a gap in the literature on preservice teachers' perceptions and beliefs about data privacy regulations and policies when considering use of social media for educational purposes. | Pre-service teachers | 148 | Mixed instruments | Right to digital education; GDPR right. |
| Marshall (2014) | To explore the ethical issues around use of MOOCs in education. | Theoretical | - | - | Protection of privacy rights in online environments; Responsibility |
| Okada, Noguera et al. (2019) | To understand teachers' views on use of e-authentication tools and how they impact confidence in e-assessment. | Teachers | 108 | Questionnaire pre-post; focus group | Digital identity rights; Protection of privacy rights in online environments |
| Okada, Whitelock et al. (2019) 2018 | To shed light on this area by examining the attitudes and experiences of 328 students who used an authentication system known as adaptive trust-based e-assessment system for learning (TeSLA). Evidence from mixed-method analysis suggests broadly positive | University students | 328 | Questionnaire (pre-post) | Digital identity rights; Responsibility |

**Table 1**
*Studies Included in the Research*

| Author & year | Aims | Participants | Sample | Instruments | DD&R Indicators |
|---|---|---|---|---|---|
| | acceptance of these e-authentication technologies by distance education students. | | | | |
| Pangrazio & Selwyn (2019) | To outline a range of salient socio-technical understandings of personal data generation and processing. | Theoretical | - | - | Right to digital security or cybersecurity |
| Park (2013) | To examine the impact of three dimensions of digital literacy on privacy-related online behaviours: (a) familiarity with technical aspects of the Internet, (b) knowledge of common institutional practices and (c) understanding of current privacy policy. | Adult Internet users | 419 | Questionnaire | Protection of privacy rights in online environments |
| Rajab & Eydgahi (2019) | To assess the explanatory power of theoretical frameworks on higher education employees' intention to comply with information security policies in higher education. | University staff | 206 | Questionnaire | Right to digital security or cybersecurity |
| Regan & Jesse (2019) | To examine the effects of Big Data in K12 education, considering the vulnerability of student privacy. | Theoretical | - | - | Protection of privacy rights in online environments |
| Rennie et al. (2019) | To identify the most frequently used applications in 148 Australian primary schools and classify them by their stated treatment of identifiable information. | Theoretical | 37 | Search processes; Interviews | Right to digital education; Responsibility |
| Selwin (2015) | To examine the importance that digital data are acquiring in education, considering the risks that purist implementation may have on learning, inequalities in access, privacy, data surveillance, etc. | Theoretical | - | - | Right to universal access; Protection of privacy rights in online environments |
| Slade et al. (2013) | To provide a socio-critical perspective on LA use, considering ethical issues that should be included to preserve students' safety. | Theoretical | - | - | Protection of privacy rights in online environments |
| Tamjidyamcholo et al. (2014) | To deepen understanding of how to influence an individual's tendency to engage in knowledge sharing behaviour in virtual information security communities and to identify the quantitative relationship between knowledge sharing and the expectation of security risk reduction. | LinkedIn groups | 142 | Questionnaire (pre-post) | Right to digital security or cybersecurity; Protection of privacy rights in online environments |

**Table 1**

*Studies Included in the Research*

| Author & year | Aims | Participants | Sample | Instruments | DD&R Indicators |
|---|---|---|---|---|---|
| Vanacker (2011) | To identify ethical issues associated with university instructors' use of plagiarism detection software (PDS), specifically the Turnitin programme. | Theoretical | - | - | Digital identity rights; Copyright; Responsibility |
| Walton et al. (2015) | To examine the online presence of a Canadian medical school graduating class by scanning students' public profiles on the social networking site Facebook, incorporate this information into an educational activity that addresses professionalism and social networking, and assess the impact of this activity on student behaviour. | University students | 121 | Content analysis in Facebook | Digital identity rights; Right to digital security or cybersecurity |
| West et al. (2020) | To explore the LA literature to determine how student perspectives are positioned as dashboards and visualisations are developed. | Theoretical | - | - | Protection of privacy rights in online environments |
| Whitelock-Wainwright et al. (2019) | To develop and validate a descriptive questionnaire that offers a robust, methodologically sound solution to measuring student expectations of LA services. | Students | 210 | Questionnaire | Protection of privacy rights in online environments |
| Williams et al. (2019) | To develop the first privacy game for (Android) Wear OS watches to encourage changes in privacy behaviour. | Students | 10 | Questionnaire; Interviews | Protection of privacy rights in online environments; Responsibility |
| Zaman (2020) | To discuss how youth-centred design efforts risk falling into three traps of privacy by design, related to: 1) the different degrees of decision power within and between child-centred design guidelines and participatory design with young people; 2) the involvement of young people in design as citizens versus consumers; and 3) the conditions under which their participation in design is empowerment rather than mere decoration. | Theoretical | - | - | Right to participate; Responsibility |