The Safety Area of Digital Competence: A Mixed Method Study in Galician Primary Education Students

Esther Vila-Couñago, Uxía Regueira, and Eulogio Pernas-Morado

***Abstract*— This article aims to evaluate the safety area of digital competence in pre-adolescents schooled in primary education as well as to understand the processes that interfere with the development of that area. A mixed research methodology was used through an exploratory sequential design with a qualitative phase (multiple case study) followed by quantitative phase (assessment test on safety). Particularly noteworthy among the results obtained is the influence of the family on the subcompetence of health protection as it is the one that worries families the most and where students score the highest on the test conducted.**

***Index Terms*— Digital competence, digital divide, digital safety, mixed method research.**

I. Introduction

THE impact of new technologies in societies has led to changes in all domains of life so that digital competence (DC) has become one of the skills demanded by contemporary society. This situation has been made all the more apparent and pressing in view of recent events marked by the lockdown and the different measures taken by governments as a result of the health crisis caused by the COVID-19. DC has now proved indispensable for teleworking, telelearning, leisure and also to keep abreast of topical matters and remain in contact with those dear to us. The risks that a number of authors have been suggesting as regard the digital divide [1], [2] are today magnified by the lack of access and competences: inequalities in terms of gender, social breakdown, institutional exclusion, socialization spaces, infoxication or social alarm, to mention but a few.

Manuscript received August 7, 2020; accepted September 8, 2020. Date of publication October 22, 2020; date of current version November 16, 2020. (Spanish version received May 12, 2020; revised June 15, 2020; accepted July 1, 2020). This work was supported by the Spanish Ministry of Economy and Competitiveness and the European Regional Development Fund (ERDF) through the Project Competencia Digital en Estudiantes de Educación Obligatoria: Entornos Sociofamiliares, Procesos de Apropiación y Propuestas de E-Inclusión under Grant EDU2015-67975-C3-1-P. *(Corresponding author: Eulogio Pernas-Morado.)*

Esther Vila-Couñago and Eulogio Pernas-Morado are with the Department of Pedagogy and Didactics (Area of Didactics and School Organization), School of Education Sciences, Universidade de Santiago de Compostela, 15782 Santiago de Compostela, Spain (e-mail: esther.vila@usc.es; eulogio.pernas@usc.es).

Uxía Regueira is with the Department of Pedagogy and Didactics, School of Education Sciences, Universidade de Santiago de Compostela, 15782 Santiago de Compostela, Spain (e-mail: uxiafernandez.regueira@usc.es).

There exists a Spanish version of this article available at http://rita.det.uvigo.es/VAEPRITA/V8N4/A17.pdf

Digital Object Identifier 10.1109/RITA.2020.3033218

In this context, a number of measures and tools have urgently been put in place in a variety of sectors, including the educational domain, so as to pursue the daily activities in this new scenario. While in the current context concerns have been voiced as regard access and instrumental competence –basic issues to ensure the continuity of the educational activity– it is paramount to maintain at the center of debate the fact that the ability to use these technologies in a clever, critical and reflexive way should be conceived within the framework of the interconnection and negotiation between the opportunities and risks they entail [3]. A negotiation that in times such as these –when there is high exposure to tools and technologies implemented with urgency and at an accelerated pace, where world-level data collection has been normalized with new purposes that add to those already known and where the focus is on health– means that e-safety and the DC on this domain are a priority.

II. Digital Competence in Pre-Adolescents: The Safety Dimension

This study has as its frame of reference the DIGCOMP Project [4], whose definition of DC mentions a learning that entails a cognitive empowerment and the transfer of knowledge through the use of digital tools in a variety of contexts [5] in a manner that is effective, efficient, suitable, critical, creative, autonomous, flexible, ethical and discerning [4] in order to solve real problems. In DC, five dimensions have been identified: information, communication, content creation, safety and problem solving. In turn, these areas encompass a total of 21 subcompetences.

It follows from the literature that the technology-related safety dimension [3], [6]–[10] is the one that worries families and institutions working with minors the most. This dimension, in turn, encompasses four subcompetences [4]:

- Device protection. It entails understanding the on-line risks and threats; knowing and being able to take security measures to protect the devices and prevent the fraudulent use of passwords; showing a positive but realistic attitude regarding the risks involved in the on-line use of new technologies.
- The protection of personal data. It involves understanding the terms and conditions of privacy as well as its guarantee and protection through safeguarding the data shared and the creation of the user's own digital identity

and those of others, preventing situations that may lead to cyberbullying.
- Health protection. It entails knowing and acting on the basis of the risks posed by new technologies as regard to psychological and physical health. It also involves the relation between one's own behavior and the wellbeing of the others.
- The protection of the environment. It involves awareness on the relation existing between technological progress and the environment, thus acting in a coherent and efficient manner.

A later version, called DIGCOMP 2.0 [11] introduced some changes to these four subcompetences. Among them, the second subcompetence changed its name to 'Protecting personal data and privacy, thus adding aspects that have to do with the understanding of how personal identification details and data are used as well as how platforms and social networks operate or the management of digital identity. Besides, cyberbullying –the on-line risk that affects to the greatest number of children between 9 and 12 [9]– is considered a subcompetence associated to health; to which the skills aimed at promoting inclusion through digital tools are added.

Current educational legislation mentions the need to tackle safety issues for a proper development of DC [12], [13]. Within this framework, safety is understood as a knowledge of the risks that technology poses as well as having at one's disposal strategies to avoid them: the protection of the information and the recognition of its additive aspects. Cyberbullying and other risk issues are not included or are considered implicit in the communication dimension. Also not included are the protection of the devices or the environment. Relevant issues such as the creation, attention to and management of digital identities, whether own or from third parties, are excluded from the curriculum. Although safety is one of the issues that worries families and institutions the most, training in this dimension of DC is still a pending task that requires further and better training [6] for a safe and responsible use of the new technologies and the Internet.

Previous research on e-safety shows awareness and good attitudes towards safety [6], [14], [15]. In the case of Spanish students, the perception of their DC in this dimension is higher than that shown in other dimensions and is above the European average [14]. However, the studies cited above show –in contrast with the students' self-perception– a low performance in practices associated with the safe and responsible use of the Internet. Young people seem to have a knowledge about risk situations and awareness about suitable practices such as: refraining from giving personal information, encouraging the protection and care of their own virtual image and that of others and showing proper behavior in digital environments as suggested by the findings of the research conducted with university students [15] and primary education [5]. In contrast with these data, practices such as the use of safe passwords or the implementation of protocols for changing them as well as maintaining usernames private are not common practices [7], [15].

Their concern for privacy is shown through the characteristics of their account or their binary conception about their 'friends', which may even be so restrictive as to undermine the potentiality of social networks [3]. Almost half of the minors between 9 and 12 years of age (45%) have a private profile [9]; and a number of studies [7], [9] show that most pre-adolescents between 11 and 12 (74%) say that they only accept friend requests from persons they know while contact with unknown people occurs through instant messaging and social networks, not in a physical space. However, in these profiles it is frequent that minors upload photographs of themselves, personal information such as surnames, telephone numbers or the school they attend [8], which means that it is difficult for them to know how to manage privacy online and digital identity.

Similarly, as far as health and the environmental impact of the technologies, studies that have been conducted with university students suggest a number of contradictions between the knowledge they have and what they do [16]: they state that they are conscious of addictions to devices, of their psychological effects or their effects on physical wellbeing but they admit to having developed dependency to these devices. Similarly, although they say they are aware of the power consumption of the devices they use and the environmental cost involved in their manufacturing, the items associated to the recycling of devices have low scores and they admit that they do not take into account the environment when they buy, replace or use electronic devices.

The data from research suggest a dissonance between the perception of DC and the practices of young people in digital contexts. Therefore, the capacity to establish a conscious negotiation between the potentialities and the risks of the Internet is called into question. While there are multiple studies that tackle digital safety, there are few studies that study the competencies in this area. Similarly, predominant studies include the perceptions of young people, but they do not assess their DC. And there are few studies that look at this issue in the context of primary education. It becomes therefore apparent that it necessary to ascertain what skills are developed, how and when they are developed and who influences this process [17]. This study, therefore, seeks to evaluate the DC in the area of safety in pre-adolescents schooled in primary education by analyzing the subcompetences and the aspects it encompasses as well as understand the processes, contexts and persons that interfere with the development of the DC in the safety domain. The research reported here is part of the CDEPI Project ["*Competencia digital en estudiantes de educación obligatoria. Entornos sociofamiliares, procesos de apropiación y propuestas de e-inclusión*"] conducted in the Autonomous Communities of Castilla y León, Galicia and Madrid.

III. METHOD

This study uses a mixed methodology research. Specifically, an explanatory sequential design [18], which combines a first qualitative phase and a second quantitative phase. In the first phase a multiple case study was made to gain a deeper understanding and an analysis of the safety of DC and, in the second phase, an evaluation test was made of the safety

area of DC adapted to the target population of the study. This methodological design makes it possible to analyze to what extent and in what way quantitative results confirm qualitative findings [18], so that the response to the objectives set is more complete and comprehensive through the integration of the results of both methodological approaches.

A. Phase 1: Case Study

This is an analytic, multiple-case study [19] with a holistic design [20], based on a comprehensive vision and understanding where each individual illustrates one unit of analysis. Following application of the principle of informed consent, a total of eight subjects (six from CDEPI-Galicia research project and two more cases that were included at a subsequent research stage) participated in the study. Their fictional names are: Alfonso (Al), Antón (An), Catarina (Ca), Lucía (Lu), Bieito (Bi), Jaime (Ja), Pedro (Pe) and Elisa (El).

Previously an *ad hoc* questionnaire was administered to 182 families from five schools in the Autonomous Community of Galicia who had children in their sixth year of Primary Education. From the data collected, participants were selected on the basis of maximum efficiency [21], encompassing family environments with different cultural capital. Specifically, two cases have a low socio-economic level (Bi and Ja), three cases have a medium socioeconomic level (Al, An and El) and three cases have a high socioeconomic level (Ca, Lu and Pe). Some of the cases share family setting as Alfonso and Antón are fraternal twins and Catarina and Lucía are identical twins.

Data collection was conducted during the second and third terms of the 2016-2017 academic year. The data collection techniques used were essentially two:

- In-depth interviews lasting approximately 1 hour with the children, their parents or their legal guardians, their teachers/tutors and, in some cases, also the school principals and even some friends of the children. Interviews were typically made in school premises, audio-recorded and fully and literally transcribed.
- Participant observation of the subjects, essentially of the behavior of the children when engaged in specific computer activities or while gaming with their laptop computer or tablet, paying particular attention to the responsible and safe use of this technology. The performance of these activities was also video recorded for subsequent analysis.

All the data collected were analyzed using the software Atlas.ti 7 following a mixed inductive-deductive procedure [22]: on the one hand, the theoretical framework provided by the DIGCOMP on subcompetences on the safety area was taken into account; and, on the other hand, new categories emerged as the data were examined, thus broadening the comprehensive framework of the categories above. As a final step in the process of analysis, several reports were given to both the families and the schools in order to contrast the information collected and thus validate the observations and interpretations made.

In the presentation of results, textual quotations of participants are included. They are identified by using the two first initials of the case and they may be accompanied by a code that designates the other people interviewed: "Ma" for mother, "Pro" for parents (both participate), "Tu" for tutor and "Ab" for grandmother. The interview number is also included.

B. Phase 2: Applying ECODIES Test-Safety Area

In this second phase, of a quantitative nature, a DC evaluation test is used that was designed by the GITE research team of the University of Salamanca –which is in charge of one of the CDEPI sub-projects on the safety area and constructed from the DIGCOMP European framework and adapted to the ages of children in their sixth year of Primary Education, consisting of 72 defining indicators of knowledge, skills and attitudes on safety-related DC [23], [24].

On the one hand, the part of test dealing with knowledge and skills on the safety area consisted of 16 items with four options where only one is correct. On the other hand, attitudes were measured using 6 items with a Likert-type scale with 5 options (1: very much disagree, 2: disagree, 3: indifferent, 4: agree, 5: very much agree). This is a one-way scale where all six items have been written in a positive way (agreeing indicates a favorable attitude).

To determine the score for each subject in the test, responses were coded in a dichotomous fashion: 1 is correct answer, 0 is wrong answer. Responses to items on attitudes are dichotomized: those on the categories "very much agree" and "agree" are coded as 1 (positive attitude) and those corresponding to "very much disagree", "disagree" and "indifferent are coded as 0 (non-positive attitude).

The test, presented in a website designed for this purpose, was administered throughout the 2018-2019 academic year to a representative sample of students in their 6^{th} year of Primary Education in public schools in Galicia on the basis of three stratification criteria 1) type of province –Atlantic or non-Atlantic–, 2) whether the school participated in a technology immersion program or not and 3) population density of the municipality –scarcely populated area, intermediate area and densely populated area–. The sample finally comprised 563 students.

The analyses of the items were made in a differentiated manner on the basis of its typology: objective test type and Likert-type scale. As to the items in the objective tests, although they include different types of easiness-difficulty, there is a greater representation of difficult questions: 2 very easy questions, 2 easy questions, 5 average difficulty questions and 2 very difficult questions. The item discrimination index based on the extreme groups approach is very good except for items 8 and 14. They were therefore removed from this study because of their excessive difficulty and little discriminative power. As to the attitude items, their suitable homogeneity was verified (correlation of the item with the total calculated as the summation of all the items except for the one under analysis) yielding values which range between 0.35 and 0.54. The reliability of the test on the safety area as a whole (dichotomized items of knowledge, skills and attitudes) in terms of internal consistency, showed an acceptable value (KR-20 = 0.77).

TABLE I
STRUCTURE ON THE BASIS OF SUBCOMPETENCES AND ITEMS

Device Protection Subcompetence
1. Knows what to do when a device is infected by a virus (knowledge).
2. Knows how to create a safe password (skill).
3. Uses the antivirus in the computer (skill).
4. Knows the rules to create passwords (skill).
17. Considers that passwords must only be shared with the parents or tutors (attitudes).
21. In public places, tries to use the WIFI when it is sure (attitudes).
Personal Data Protection Subcompetence
5. Knows that once you publish something on the Internet, control is lost over it (knowledge).
6. Knows the consequences of your password being found out (knowledge).
7. Identifies the publications that may jeopardize the privacy of their personal details (skill).
19. Considers that uploading photos onto the Internet and share personal and family information may be dangerous (attitudes).
Health Protection Subcompetence
9. Knows how to prevent cyberbullying (knowledge).
10. Plays *online* with friends in a positive way (skill).
11. Maintains a correct posture when using digital devices (skill).
12. Navigates the Internet without wasting time (skill).
16. Is able to stop playing if they feel nervous (skill).
18. Is aware that technologies can be addictive (attitudes).
Environment Protection Subcompetence
13. Knows that the consumption of devices that has an impact on the environment (knowledge).
15. Saves energy when using devices (skill).
20. Appreciates the technological devices that respect the environment (attitudes).
22. Is aware that the natural resources used to manufacture mobile phones are limited and may exhausted (attitudes).

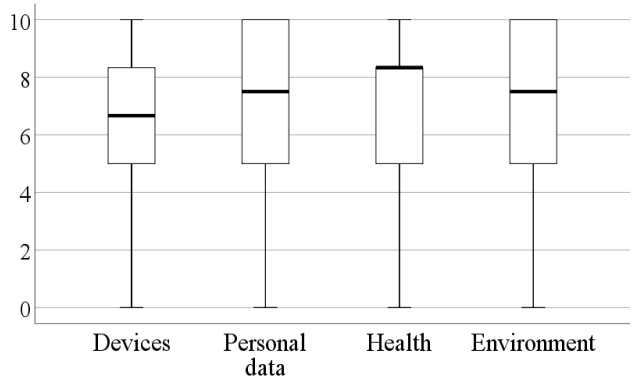

Fig. 1. Distribution of the responses in the safety area subcompetence.

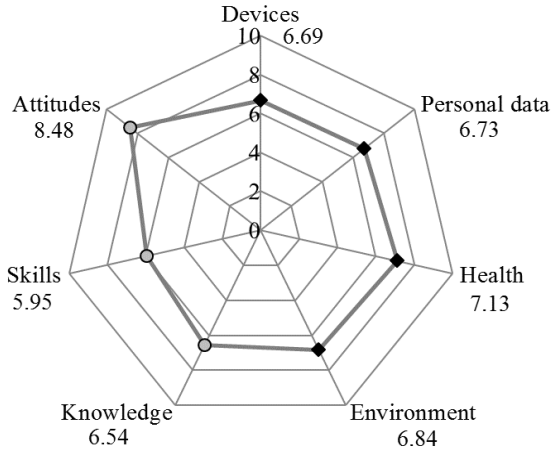

Fig. 2. Average scores obtained in the subcompetencies (rhombus markers) and the aspects (circle markers) in the safety area.

For this study, the items in the safety area of the ECODIES test were rearranged so that each subcompentence includes items of knowledge, skills, and attitudes in accordance with the DIGCOMP model. The structure used is shown in Table I.

The scores obtained at each of the subcompetences are the result of adding the number of correct answers in the corresponding items. These scores were calculated on a base 10 number system to be able to make comparisons among the subcompetencies. Furthermore, the scores for the three aspects of the DC in the area of safety were calculated: (5 items), skills (9 items) and attitudes (6 items).

Univariate descriptive analyses were conducted (percentages, central tendency measures and dispersion measures), using the SPSS statistical package, version 25. Besides, due to the lack of normality in the distribution of the responses –verified through the Kolmogorov-Smirnov test (Sig. = 0.00)– the Friedman test was used to determine whether there were significant differences between the different subcompetences and aspects of the DC safety area.

IV. RESULTS

Upon evaluating the safety area as a whole –using the ECODIES test– the students' scores reflected a medium level (X = 6.86; S = 1.91; Md = 7.50). The subcompetence that students have developed the most is that associated to the protection of the health (X = 7.13; S = 2.48). As shown in Fig. 1, their responses are concentrated to a greater extent in the highest scores (Md = 8.33). In the remaining subcompetences lower average scores were obtained (see Fig. 2), in this order: protection of the environment (X = 6.84; S = 2.70; Md = 7.50), personal data (X = 6.73; S = 2.89; Md = 7.50) and devices (X = 6.69; S = 2.26; Md = 6.67). Significant differences between device protection and health protection subcompetences (Sig. = 0.00) and between personal data protection and health protection (Sig. = 0.03) were found.

As to the DC aspects, the highest scores were obtained in the items attitudes (X = 8.48; S = 2.13; Md = 10), as reflected in Fig. 2, whose response distribution is very homogeneous (see Fig. 3): 75.5% of students scored between 8.33 and 10. The lowest scores were obtained in the knowledge items (X = 6.54; S = 2.92; Md = 6) and skills (X = 5.95; S = 2.29; Md = 6.67). Among the three aspects analyzed there are significant differences (Sig. = 0.00 in the three contrasts).

A. Device Protection Subcompetence

Of the three "cores" that make up the device protection-related subcompetence (management of passwords, protection

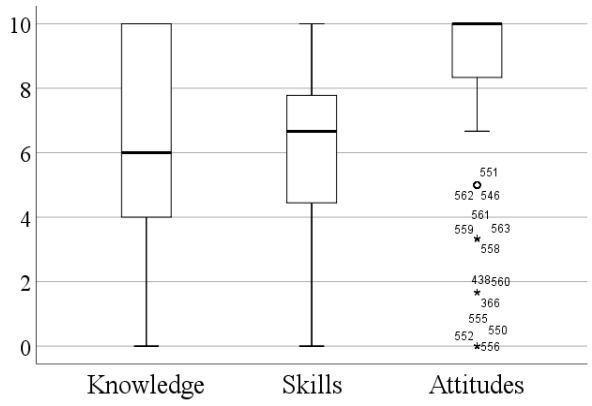

Fig. 3. Distribution of the responses in the DC aspects of the safety area.

against virus and access to WIFI networks), the need to run the antivirus (item 1) is the one with the highest percentage: 81.7% of the students know that when a device is infected with a virus the antivirus must be immediately run. Results fall dramatically as regard to virus prevention as only 52.9% admit that every so often they open the antivirus and scan the hard disk (item 3), while a worrying 16% does not use antivirus software as they have never need it.

The cases show an evident duality that is consistent with the data collected through the ECODIES test, as they understand that they must run the antivirus as soon as the equipment is infected on the one hand, but, on the other hand, they are careless in preventing against computer viruses. This contradiction is already seen in the family context: the parents of Catarina do not even know whether the equipment their daughter uses (which is provided by the school) has an antivirus installed: "*I am under the impression that that is not something that depends on her…* (…) *I've never heard them speak of any of this…*" (Ca_Pro-2). And the same is true of Pedro's parents, who have a lot of confidence in their son's skills "*He downloads, installs, deletes, updates…*" (Pe-1), but they admit that he has not installed any antivirus and that he is not familiar with the maintenance of the computer. They contradict themselves when in the same interview they say that actually the antivirus "came pre-installed with the computer" as they (his parents) took an interest in these matters. The testimonies of both families –with a high sociocultural level– contrast with the evident concern regarding the use their children make of digital technologies when other areas of DC are brought up.

Particularly noteworthy is the situation of Antón whose computer *"caught a virus"* (An-1), while his father downloaded music (in the computer owned by the children, not in the one supplied by the school). This could be a frequent occurrence as the mother wryly remarked that he is an "*expert in downloading viruses*" (An_Pro-2). And when he remarks "Actually…*Linux is free from viruses*" (An_Pro-2), when speaking about the laptop supplied by the school (that runs on Linux) he shows that he has little knowledge on the matter.

Some cases reveal a lack of knowledge or concern on this issue. For instance, Elisa causally admits that she has a virus in her computer when showing the interviewer the procedure she follows to download videos or she mistakes an antitheft app called Cerberus, which she found pre-installed in her mobile phone, for a proper antivirus.

On the other hand, the management of passwords – the second of the cores mentioned within the device protection subcompetence– had rather discouraging results in the ECODIES test as far as safety is concerned: only 46.5% selected a safe password for their device (item 2), specifically the initials of their favorite singer and the year s/he was born; while the rest (over half of them) would opt for clearly less safe options (from their ID card number to their own name, date of birth or their home address). Results improve as regard to the norms they follow to create passwords (item 4): 60.9% select passwords with many different types of characters as opposed to 24.2% that opt for short ones (as they are easier to remember), 8.3% use only lowercase or 6.6% use only letters.

If we look at cases, only Elisa clearly states that she has a "*very difficult*" password, so much so that she does not even mind that the interviewer sees her type it "*because it has a lot of letters*" (El-2). But these cautions may not be very useful as the girl confesses to the interviewer that she has all her passwords noted down in her mobile phone case, although "*she knows them by heart*" (El-2). Nobody knows that she has them there, not even her parents (she herself hardly remembered it because she had noted them down there a long time ago).

Lucía, on her part, seems to prioritize the need for a simple password *"otherwise, we would forget it"* (Lu-2). Besides, she uses the same password for her WIFI and for her email, instead of prioritizing her safety using a safer combination.

As to attitudes (item 17), a high percentage (75.5%) agrees or very much agrees with sharing passwords only with their parents or tutors, as opposed to 15.1% who disagree or very much disagree. If we look at the cases, we see that Anton's mother confirms that her children tell her their passwords. Lucía also shares her passwords with her parents and the teacher as well as with her twin sister, Catarina. But whereas Lucía says that her classroom mates do not know the passwords of the others, Catarina admits that passwords are shared among friends.

Jaime is ambivalent: it is fine for him that his father knows his passwords –he spends some afternoons video gaming with him– and he is perfectly aware of the risks of sharing a password with someone else, even if that someone is an online gaming "*friend*", "*because maybe later they may take my account, delete games, I don't know*" (Ja-1) even if this might have advantages such as advance to the next level. However, as far as the measures he takes as regard his passwords in other devices, like his computer, Jaime does not seem to be so cautious and says that he does not use them. Elisa, on her part, is aware of the fact that sharing her passwords with her schoolmates involves risks: "*they may log in and hack it, for instance*" (El-2), although she admits that she knows some of her schoolmates' because "*they wouldn't keep them to themselves*".

Lastly, as to WIFI access, which is the third core of the device protection subcompetence, it shows a high percentage, 83.7%, as regard the use of WIFI in public places when it

is safe, whereas 5.6% disagree or very much disagree. In this regard, we are only aware of one instance of access to a public WIFI network for the whole of the cases studied, namely that of their schools, probably the only one most of the students participating in ECODIES are aware of. This might have had some impact on the results as they do not have any reason not to trust the safety of their passwords in spite of the fact that their structure is quite predictable for every student in the same class, which makes it quite easy for any of them to figure out their classmates' password: "*everyone knows it*" (Pe-1). WIFI is seldom mentioned and when they do concerns are not so much about safety as about connectivity problems in the schools as it became apparent when trying to connect Jaime's equipment during an interview or as Pedro and his family remark.

B. Personal Data Protection Subcompetence

The issues addressed revolve around the perceived control on the part of students regarding what they publish on the Internet, the privacy configuration of their accounts, the consequences of other people knowing their passwords and the type of contents that endanger their identities if uploaded.

50.4% of students know that once you upload something on the Internet, whether they are photographs or data on their family or home, control is lost over them (item 5). On the other hand, 26.3% consider that it is them who control the information and that they can delete it whenever they want; 18.5% believe that the contents they upload will only be seen by their actual friends and 4.8% believe that this information has no relevance whatsoever for their future or that of their families.

According to Catarina and Lucía's teacher/tutor, most of her students have their own Facebook and Instagram accounts "*despite the fact that a few days ago there was …well, a Civil Guard officer came to speak about safety on the Internet and told them that they could not have an account until they turned fourteen*" (Ca_Tu-1). Students do not know that there is a minimum age limit to register with the platforms or they consciously violate the terms and conditions of use of these services by creating a profile with fake data or based on someone else's data: "*Sure, they try… then they start by providing my data and then they say ≪this is working, let's do it with ours≫"* (An_Ma-1). Besides, students show that their knowledge and skills about account privacy configuration are very basic. Elisa even had a personal profile in Google+, without being aware that it was public: *"the surprise came because of a WhatsApp message she had ≪I have this many followers≫ (…) Then, we saw that it was public, that* [it] *could be accessed"* (El_Pro-1).

The contents uploaded by students to the Internet are mediated by the family context. On the one hand, there are families, like that of Catarina and Lucía, that deny them access to digital environments. The same is true in the case of Pedro: *"It's a rule. They will not allow me until I'm, I think, fifteen or fourteen"* (Pe-1). Bieito's family have also strictly prohibited their use. His middle sister, who is 13, disobeyed and the resulting punishment: she had her Instagram account closed and four weeks with no access to her mobile phone. On the other hand, there are families like Elisa's or Antón and Alfonso's who allow the use of social networks but they strictly prohibit their children from uploading personal photographs –although the parents are not fully aware of all the applications and networks that their children use–: "*Sure, They would ask me… ≪Mom, can we do such and such…?≫ And I would say: ≪Look, you're with the computer all the same … so you may as well do it. Mind you, try not to upload photos of you…≫*" (An_Ma-1).

As to the consequences of other people finding out their personal passwords, the quantitative study shows that 65.2% of students do know them and they know that they may be used to send messages by someone pretending to be them, read the messages they have received from any of their contacts or even change the password so that they cannot access their own messages (item 6). The case study has led us to identify how this awareness has little effect on the passwords for the E-Dixgal platform used in the school environment as the general assumption is that it does include any sensitive content and that is the same for the whole group-class. However, for the accounts associated to other digital platforms and social networks that students use outside the school environment, there is indeed greater awareness of the potential consequences of disclosing their password or that other people may come across it or figure it out: "*They may upload a photo that you don't want uploaded*, *for instance*" (El-2). Elisa, despite the fact that she knows the passwords of some of her schoolmates, understands and respects their privacy: "*I wouldn't like anyone logging on to mine"* (El-2).

In the case of Bieito, however, he has no digital accounts of his own. Interestingly enough, he uses legacy Gmail accounts – through the mobile phone he has been given, where no factory data reset was performed–. He, therefore, opens the emails addressed to the former owner of the phone, thus violating the privacy rights of the other person without being aware of the legal implications of his acts.

The quantitative study also reveals that 61.8% of students can identify what contents may pose a threat to their identity (item 7), like for instance a photograph at the front door of the house where the number and name of the street can be seen, a blog entry that includes a telephone number or a photograph from last summer holiday. However, there is a 30 percentage-point increase (91.7%) in the students who believe that uploading photos to the Internet and sharing personal and family information may be dangerous (item 19), with 8.3% disagreeing or showing an indifferent attitude towards this fact.

In this regard, Elisa takes certain precautions in the dissemination of her image and is aware of the importance of the privacy of personal data on the Internet: "*this is the photo I have, isn't it?* [she is speaking of an email account] *I′m not seen, that's on purpose, I just show my back"* (El-2). She has the habit of googling herself to make sure that there is not an image of herself where she can be identified. It is found that all this zeal originates in parental control and the concern to ensure the protection of her personal data and prevent any danger that might result from sharing information: *"All her*

videos are private [videos she creates with the application Musical.ly] *(…) Because you don't know who may watch it. Or what for"* (El_Pro-1). But, sometimes, Elisa is not cautious: "*yes, my face is seen but it is not that important* [speaking of her Instagram profile photo]" (El-1). A carefree attitude that she adopts in other behaviors such as visiting unsafe websites to download songs where pop-ups and banner ads are constantly being displayed, which she identifies as negative without being aware of the risks they pose.

Pedro is perfectly aware of what personal information should not be given on the Internet although he inconsistently uses his Gmail account to subscribe to games and YouTube channels. Occasionally, he seems to be more aware of personal protection data and to access some game he even provides email accounts that do not exist. When communicating with his clan members through the chat within Clash Royale and Clash of Clans he notes "*We don't say anything personal, nothing"*, "*We don't even say our names*" (Pe-1). Besides, he elaborates on the risks of providing personal information on social networks as there is the risk of falling into dangerous viral challenges: "*It is called the "The Blue Whale Challenge", (…) to accept it you need to give your full name and your address and… if you do not complete the challenge, they'll kill your family*" (Pe-1).

On his part, Jaime verbalizes that he is aware of the risks the Internet poses. Indeed, he does not use his own name in his YouTube o GTA accounts, but when asked about the specific motive to do so he does not provide a clear argumentation on the issue: "*I don't know, I've just never given my name"*, *"Everybody uses made-up names"* (Ja-5). This suggests that this habit has more to do with configurating his identity as a gamer than with online safety.

Lastly, Alfonso and Antón are aware of the need of protecting their personal data, with some qualifications, though. In one of our interviews with Alfonso, he showed us his Instagram, and he noted that he was worried about a photograph of a third party that he had uploaded in this private profile: "*I need to delete a photo because according to Laura* [fictitious name], *there is this girl that can report me for uploading a WhatsApp photo*" (Al-1). Whether it was because he does not know how to do it or because he forgets, this photo remains undeleted throughout the various interviews held with him.

The cases studied show therefore a lack of consistency between what they believe and say and what they actually know and do, in keeping with the results in the ECODIES test, as indicated: higher scores in attitudes (item 19) than in skills (item 7).

C. Health Protection Subcompetence

This has to do with the skills required to ensure psychological wellbeing, which encompasses the quality of the relations established online, the time spent online and its quality as well as physical wellbeing.

In the case analysis, it can be observed that the main concern of the families as regard this subcompetence has to do with the space-time variable. It appears across the board in all cases as a norm, a specific behavior by some member of the family or through discourse; and it is this variable that has greater weight in the physical and psychological safety of the children. It is most noticeable in the cases of a medium socioeconomic capital where the issue of access and the concern for time is a constant in the discourse. Elisa's family has put in place strict norms for its control, stating that *"On weekdays she doesn't have her mobile, she is given it on Friday after school and I take it away between meals"* (El_Pro-1). Antón and Alfonso's family also restricts its use during the week. Although less strict rules apply, sometimes they are not complied with and parental control tools have been installed that limit exposure time, *"Because otherwise they would be on non-stop (…) the home mobile has … parental control on, basically to prevent them from being online all the time"* (An_Pro-1).

In spite of the fact that there are not always explicit norms to ensure when and for how long they can be online in all families, there is some sort of control by some relative like in the case of Bieito, whose sister intervenes and takes the device away from him given the lack of competence in the home, which results in lenient rules: *"No, I ask grandpa and he lets me use it* [speaking about the console]. *Not on weekdays"* (Bi-2). Even in the case in which the device is not taken away, there is an explicit reflection around the time allowed online that is the result of striking a balance between the potentialities of these technologies and the risks that are identified. Jaime's family does not identify enough risks to limit playtime, which they consider positive for his ADHD (Attention Deficit Hyperactivity Disorder). A decision that leads to a discussion between his mother and his school tutor.

In families with a high sociocultural capital, the concern is focused on the manner in which devices are used. Their emphasis is on trying to ensure that the time spent on these devices has a positive impact on the development of the children while reducing or dispensing with other potential uses. This is shown in the restriction that applies in the case of the twin sisters consisting in not allowing any non-academic use with the sole exception of some mini games they sporadically participate in or when contacting with their extended family. In the case of Pedro, this is shown in the supervision and the encouragement of other uses, allowing access to entertainment and some specific games, but not to social networks.

Cases show a concern about whether or not this use conflicts with other duties such as studying; or whether its excessive use may lead to negative consequences for the children. Similarly, the ECODIES test reveals that students are aware of the potential for addictions that these devices have. 90.2% of the students admit that they are aware that technologies may create additions (item 18) and only 9.8% disagree or are indifferent to this statement.

Whether families articulate rigid and sophisticated norms, like in the case of Elisa, or they consider that the risk-benefit balance is positive and therefore no intervention is necessary, like in the case of Jaime, no reference is made by the children themselves when adjusting time spent online that is based on the consideration that they devote too much time or on

the feeling that their behavior might have addition-related elements.

According to the results of the ECODIES test, 63.6% of students are able to stop playing if they are feeling nervous (item 16). On the other hand, 16% continue to play as they consider that a bit of stress and nervousness is good to improve their performance in the game; 8.2% continue to play although their performance decreases and 12.3% would never stop playing for this reason. Similarly, as to fair play, 82.1% of the students play games with friends online positively (item 10), as they are able to maintain good relations with them even when they are losing the game.

The girls in the case studies are not gamers and if they play any video game they tend to opt for symbolic games (Elisa, 'imagines she is') or behaviorism-based solving activities (twins, puzzles and Tetris) that do not entail pursuing a problem or a target that needs to be solved strategically. These games are unlikely to lead them to online gaming (Elisa, Just Dance in the Wii, with no camera). In the case of young male players, they often collaborate or compete with other people (Jaime with the GTA or the twin brothers and Pablo with Clash Royale); and in this practice, skills associated to the management of nervousness and fair play can be seen. Jaime remarks that his cousin "*sometimes he gets mad and throws the control to the ground"* (Ja-3) and adds that he does not behave in that way although he gets angry if he does not manage to "*pass to the next phase"*, he says "*I'm gonna play with the* tablet" (Ja-3) to relax.

It is observed that online gaming interferes with the tensions existing in the families between safety and control, thus invoking the feeling of vulnerability of the children in a virtual context. Interacting with strangers brings about mixed feelings among the families. Some families value the experience of being able to approach other people and different cultures: *"he told me: ≪mom, you know I met this Mexican boy and he told me that in this country things are this or that way≫"* (Ja_Ma-1), which is interpreted as a learning opportunity: *"Sure, he is picking up some learning, then why should I restrict that? I'd rather he is, for instance, talking online with these children he can learn something from instead of watching … Shin Chan on TV"* (Ja_Ma-1). Other families emphasize the risks underlying this behavior and opt for forbidding conversations with strangers whether while gaming or on the social networks. In the case of Elisa's family, this concern goes as far as controlling the conversations the girl has through her devices: *"we try to see all her messages. We have agreed with her that she cannot delete messages (…) and that we need to know the passwords and be able to access everything on her mobile"* (El_Pro-1); and the prohibition of playing online using the microphone and the camera: *"we don't like that… they might use the camera* [to record her…]*… mightn't they?"* (El_Pro-1).

Family intervention is focused on whether to allow or forbid this behavior. This decision is the result of striking a balance between the potentialities and risks of this behavior, but it does not take into account what information children have in order to differentiate between people they know, acquaintances, and strangers. Although in some cases, like Pedro's, some guidelines are made explicit regarding the protection of personal data in online videogames, the notion 'stranger' is somehow ambiguously presented and it may be observed that each of the children generates their own strategies to discern who they can trust and who they should not. Antón and Alfonso seem to look differently at those strangers with whom they share interests, and they indeed communicate with them in online gaming chats *"don't know the people. But I like them…"* (An-1); and those unknown people with whom they apparently do not share a common interest, which grants them the status of "stranger". Elisa, on the other hand, takes the age of the person and their friends as the criterion to tell acquaintances from strangers. For her, a stranger is not someone she does not know personally but a person she considers potentially dangerous. Therefore, she accepts as acquaintances persons of her age that seem to go to the middle school she will be attending next year or those that are friends with her friends or acquaintances. She blocks those people who try to interact with her that do not fit these rules, *"some time ago, one… one mm I don't know who they were because there were two people on the photograph and she goes: ≪Hi≫. And I say: ≪Who are you?≫ ≪Someone, how're you?". And I, I don't have you, there are two people, so they are quite old. I not gonna… and I blocked'em. (…) Besides the photo there was also a rather old man … he must be thirtysomething and had a girl next to to him and I … they are no kids or anything like that"* (El-1). Although this strategy may be useful, she does not consider that the digital identity she sees on the web may be simulated. She admits that "*they have to write for instance ≪I am xxx from* [she cites as an example the name of nearby parishes and the school]*… we went together to the kindergarten≫. If they tell me that then I may believe it"* (El-1).

Children use these strategies to protect themselves and they consider them valuable and useful. This is consistent with the results of the tests, where 68.7% of the students know how to prevent harassment problems on the Internet (item 9), as they do not trust the people they do not know and who want to contact them. But the ambiguity around who is unknown suggests that the knowledge and skills they have on this regard might be weak and expose them to potential deceit. Besides, this code never comes up at school, nor is it mentioned in the interviews with the tutors; it can only be sensed that the tutor of Catarina and Lucía might have provided some information on this regard as she speaks of a talk given by the Civil Guard. The legal approach to what might be a crime would justify identifying the unknown person someone distrusts provided one has prior notions about who might be a potential offender.

As to the use of time, the test shows that 57.5% of students waste no time while navigating the Internet (item 12), going directly to the information they need to end as soon as possible. However, 14.9% tend to spend a lot of time on the Internet because they come across funny websites that keep them entertained; 11.9% end up reading or watching videos that have nothing to do with the information they were looking for and 15.6% of students usually visit many pages but do quite find what they were looking for. On this regard, there are few explicit mentions in the case studies although some mentions

have to do with navigation through hyperlinks in platforms like YouTube. In the case of Elisa this behavior is frequent. She even remarks that the contents she consumes are those recommended to her that she finds in another videos.

Similarly, references to physical health are scarce. Although 65.9% of students have a correct posture while using digital devices (item 11) –according to the data collected by the ECODIES test–, both at home and at school or with their peer group, this safety concern comes second to other health-related issues.

D. Environmental Protection Subcompetence

This subcompetence has the second highest average scoring in the safety dimension. By contrast, there are no explicit references to this subcompetence by either the children or their parents and their tutors, which means that this subcompetence is not given the same importance as others which spark an intense debate.

According to the ECODIES test, 61.1% of students know that the use of electronic devices has an impact on the environment as this refuse is difficult to recycle (item 13). 44.6% of students know how to save energy when using the devices (item 15), so that when they are doing an assignment on the computer and need to be away for some time before completing it, they use the option 'suspend' to save energy. On the contrary, 19.5% of the students leave the computer on because they will be back soon; 29% opt for switching off the screen and 6.9% leave the computer on without questioning this action.

86.5% of students are appreciative of the technological devices that respect the environment (item 20). Specifically, 61.5% and 25% of students respond 'strongly agree' and 'agree' respectively. Similarly, 81.5% of students are aware that the natural resources used in the manufacturing of mobiles are limited and may be depleted (item 22). By contrast, 18.5% of the students are indifferent or disagree with this issue.

It can be observed, in the attitudinal domain, that the variable of environmental impact is not considered when replacing an electronic device. Elisa expresses her desire to replace her mobile phone, which she has owned for one year, for a better one although it can be surmised from her own remarks and the observations made while she uses her phone that the current one is in perfect working condition. She does not even seem to have arguments to justify her choice of the new phone she wants to buy beyond social pressure towards consumerism or owning high-end devices: *"The one everyone wants (…) is the iPhone*" (El-3). The girl even estimates the price of the new mobile phone if she chooses the highest-end phone within the financial means of her family, "*I want the 6 Plus (…) because I don't like the 7 and the 5 seems too small*" (El-3), without considering or being fully familiar with the specifications of the device she wants to buy. Consequently, at no time is environmental awareness mentioned as a reason for not replacing the device, or the electrical consumption of the device as an election criterion for the new phone.

Economy plays an antagonistic role in the families with a lower socioeconomic capital, resulting in positive practices for the environment such as the 'hand-me-down' devices (which we have called "digital inheritance"). In the case of Bieito and his mobile phone *"His… it was his uncle's, his godfather's… he gave it to him. It had the card..., it was used* (…) *It must've been a year ago, if not less"* (Bi_Ab-1). While this practice does help the environment, it is not deliberately and consciously done but it is the consequence of a lack of financial resources to buy new devices.

V. Conclusion

The results obtained in both the ECODIES test and the case study reveal that students have much greater willingness (attitudes) than actual knowledge and skills on safety-related issues. Health protection stands out as the subcompentence they have a better mastery of and, likewise, it is the one that concerns parents the most, which shows the influence of families on the development of the children's DC.

The concern families have regarding the protection of health does not originate in a high DC but in the parental concern for protecting their children [25], which leads families to intervene almost instinctively by focusing on specific phenomena with media repercussion (addiction, sexting, cyberbullying…), without realizing that there is a whole set of safety-related practices that favor or promote these phenomena (net privacy, viruses, password management…). The family discourse materializes in positive attitudes on the part of the children but there are some gaps, some contradictions when it comes to practical application as well as conceptual ambiguities that emerge in both the cases and the results of the test.

Judging from the information extracted from the data analysis, school does not ensure the development of this area either. It neglects the safety of the devices they use in the classroom as regard both the use of antivirus software and the use of passwords or WIFI access. Privacy and safety are transferred to other institutions like law enforcement agencies that visit schools to provide information which is presented from a legal point of view or is focused on crime prevention. And the protection of the environment is not envisaged in the curriculum as part of DC. In fact, throughout the interviews this environmental-related subcompetence on the protection of the environment has not emerged strongly, and therefore, we have not looked into it deep enough, this being a limitation of our study that should be looked at more closely in future research. From all of the above it follows the need to explicitly and fully include the safety area of DC in curricular legislation while, at the same time, attention is paid to all factors – whether of a personal, organizational or economic nature– that enable a systematized development of this safety area in the teaching-learning processes. Besides, it would be interesting to extend the study to later educational stages such as secondary school because of the impact of adolescence on adult life as well as on the intellectual, social and affective development of individuals.

This study questions the ability of children to use new technologies in a clever, critical and reflexive way [3] as far as safety is concerned and it underscores the influence of the family environment as opposed to the school environment in

the development of DC, thus promoting the digital divide and inequality [1], [2]. These are unsettling conclusions in these times which invite to rethink the place that DC should occupy in schools once the crisis is over.

REFERENCES

[1] A. Alonso-Ferreiro, U. Regueira, and M.-H. Zapico-Barbeito, "Actitudes de alumnado preadolescente ante la seguridad digital: Un análisis desde la perspectiva de género," *Revista de Educación a Distancia (RED)*, vol. 19, no. 61, pp. 1–29, Nov. 2019.

[2] A. Gewerc and F. Fraga-Varela, "Competencia digital e inclusión social: Cuando las condiciones socioculturales se imponen," in *Competencia digital y preadolescencia. Los desafíos de la e-Inclusión*, A. Gewerc and E. Martínez-Piñeiro. Madrid, Spain: Síntesis, 2019, pp. 21–42.

[3] S. Livingstone and I. literacy, "Young people's negotiation of new online opportunities," in *Unexpected Outcomes and Innovative Uses of Digital Media by Youth*. (MacArthur Foundation Series on Digital Media and Learning), T. McPherson, Ed. Cambridge, MA, USA: MIT Press, 2008, pp. 101–121.

[4] A. Ferrari, "DIGCOMP: A framework for developing and understanding digital competence in Europe," *Joint Research Centre, Institute for Prospective Technological Studies*. Luxembourg City, Luxembourg: Publications Office of the European Union, 2013.

[5] A. Alonso-Ferreiro, *Competencia Digital y Escuela. Estudio de Caso Etnográfico en dos CEIP de Galicia* Santiago, Spain: Universidade de Santiago de Compostela, 2016.

[6] F. Annansingh and T. Veli, "An investigation into risks awareness and e-safety needs of children on the Internet," *Interact. Technol. Smart Edu.*, vol. 13, no. 2, pp. 147–165, Jun. 2016.

[7] J. Byrne, D. Kardefelt-Winther, S. Livingstone, and M. Stoilova, *Global Kids Online Research Synthesis 2015–2016*. New York, NY, USA: Unicef, 2016.

[8] J. Fernández-Montalvo, A. Peñalva, and I. Irazabal, "Hábitos de uso y conductas de riesgo en Internet en la preadolescencia," *Comunicar, Revista Científica de Comunicación y Educación*, vol. 22, no. 44, pp. 113–121, 2015.

[9] M. Garmendia, E. Jiménez, M. A. Casado, and G. Mascheroni, *Net Children Go Mobile: Riesgos y Oportunidades en Internet y el uso de Dispositivos Móviles Entre Menores Españoles (2010–2015)*. Madrid, Spain: Red.es/Universidad del PaísVasco, 2016.

[10] S. Livingstone, *EU Kids Online: Findings, Methods, Recommendations*. London, U.K.: EU Kids Online, 2014.

[11] S. Carretero, R. Vuorikari, and Y. Punie, *The Digital Competence Framework for Citizens. With Eight Proficiency Levels and Examples of use (No EUR 28558 EN)*. Luxembourg City, Luxembourg: Publications Office of the European Union, 2017.

[12] *Orden ECD/65/2015, de 21 de Enero, Por la que se Describen las Relaciones Entre Las Competencias, Los Contenidos y Los Criterios de Evaluación de la Educación Primaria, la Educación Secundaria Obligatoria y el Bachillerato, Boletín Oficial del Estado*, vol. 25. Madrid, Spain: Ministerio de Educación, Cultura y Deporte, 2015.

[13] *Consellería de Cultura, Educación y Ord. Univ., Decreto 105/2014, de 4 de Septiembre, Por el que se Establece el Currículo de la Educación Primaria en la Comunidad Autónoma de Galicia, Diario Oficial de Galicia*, vol. 171. Santiago de Compostela, Spain: Xunta de Galicia, 2014.

[14] *Survey of Schools. ICT in Education. Bechmarking Acces, Use and Attitudes to Technology in Europe's Schools*, ESSIE, Publications Office Eur. Union, Luxembourg City, Luxembourg, 2013.

[15] M. J. Gallego-Arrufat, N. Torres-Hernández, and T. Pessoa, "Competencia de futuros docentes en el área de seguridad digital," *Comunicar, Revista Científica de Comunicación y Educación*, vol. 27, no. 61, pp. 57–67, 2019.

[16] B. Castillejos, C. Torres, and A. Lagunes, "La seguridad en las competencias digitales de los millennials," *Apertura*, vol. 8, no. 2, pp. 54–69, 2016.

[17] E. Martínez-Piñeiro, A. Gewerc, and A. Rodríguez-Groba, "Nivel de competencia digital del alumnado de educación primaria en Galicia. La influencia sociofamiliar.," *Revista de Educación a Distancia (RED)*, vol. 19, no. 61, pp. 1–25, Oct. 2019.

[18] J. W. Creswell and V. L. Plano, *Designing and Conducting Mixed Methods Research*, 3rd ed. Thousand Oaks, CA, USA: Sage, 2018.

[19] X. Coller, *Estudio de Casos*, 2th ed. Madrid, Spain: CIS, 2005.

[20] R. K. Yin, *Case Study Research. Design and Methods*, 4th ed. Londres, U.K.: Sage, 2009.

[21] R. E. Stake, *Investigación Con Estudio de Casos*, 5th ed. Madrid, Spain: Morata, 2010.

[22] J. C. Tójar, *Investigación Cualitativa. Comprender y Actuar*. Madrid, Spain: La Muralla, 2006.

[23] A. García-Valcárcel. (2019). *Modelo de indicadores para evaluar la competencia digital de los estudiantes tomando como referencia el modelo DIGCOMP (INCODIES)*. Accessed: Jan. 6, 2020. [Online]. Available: https://gredos.usal.es/jspui/handle/10366/139409

[24] A. García-Valcárcel Muñoz-Repiso, L. Salvador Blanco, S. Casillas Martín, and V. Basilotta Gómez-Pablos, "Evaluación de las competencias digitales sobre seguridad de los estudiantes de Educación Básica," *Revista de Educación a Distancia (RED)*, vol. 19, no. 61, pp. 1–34, Nov. 2019.

[25] D. Buckingham, *Crecer en la Era de Los Medios Electrónicos*. Madrid, Spain: Morata, 2002.

Esther Vila-Couñago received the B.Ed. degree in pedagogy and the Ph.D. degree in education from the Universidade de Santiago de Compostela (USC). She is currently an Assistant Professor with the Department of Pedagogy and Didactics (area of didactics and school organization), School of Educational Sciences, USC. She has contributed to journals that focus on educational measurement and evaluation and to research projects on professional counseling, school quality programs, written language competence, and digital competence in compulsory education students.

Uxía Regueira received the B.Ed. degree in pedagogy from the Universidade de Santiago de Compostela (USC). She is currently pursuing the Ph.D. degree with USC within the framework of equity and innovation in education. Her research interests include educational technology, digital competence, and gender involvement in technological appropriation. She has participated in a national project. She has published a chapter of a book and two articles and has presented a number of papers at conferences with an impact on the educational field.

Eulogio Pernas-Morado received the B.A. degree in philosophy and educational sciences in 1991. He is currently a Primary School Teacher. He is a Professor with the Department of Pedagogy and Didactics, USC, and the Director of the *Innovación Educativa* Journal. A member of Grupo Stellae since its creation, he has published a number of articles, books, and other publications focused on technologies applied to education, virtual teaching and learning environments as well as didactic materials and resources.