

# Digital Citizenship is the Foundation of Cybersecurity Education

Isabella Corradini<sup>1,\*</sup>, Enrico Nardelli<sup>2</sup>

<sup>1</sup>Themis Research Center and Link & Think Research Lab, Italy.

<sup>2</sup>University of Rome "Tor Vergata" and "Laboratorio Informatica e Scuola", CINI, Italy.

**How to cite this paper:** Isabella Corradini, Enrico Nardelli. (2022). Digital Citizenship is the Foundation of Cybersecurity Education. *The Educational Review, USA*, 6(10), 601-608.  
DOI: 10.26855/er.2022.10.015

**Received:** September 23, 2022

**Accepted:** October 20, 2022

**Published:** November 22, 2022

**Corresponding author:** Isabella Corradini, Themis Research Center and Link & Think Research Lab, Italy.

**Email:**  
isabellacorradini@themiscrime.com

---

## Abstract

Cybersecurity is a very hot topic for all countries, given the increase of cyberattacks and their negative effects on the general economy. Traditional approaches tend to manage cybersecurity essentially through technological solutions, which however guarantee only short-term effects. Actually, investing in people's education represents the key driver to handle such a complex issue effectively and when it comes to school education, teaching digital citizenship is fundamental to empower children to move responsibly and safely in the digital world. In this paper, we present a study investigating the awareness actions deployed by Italian teachers belonging to primary and secondary schools in order to develop digital citizenship for their students, in accordance with a specific law that has introduced the teaching of digital civic education into the Italian school system. Answers were provided by 1,008 teachers coming from all over the country and belonging to primary and secondary schools, participating in a national project whose goal is to spread basic knowledge in informatics and educate students to a proper use of digital technologies. The results show how teachers are very active in implementing specific actions aiming at developing their students' digital citizenship. At the same time, they expressed the need to be supported for improving their actions addressed to students. Finally, they provided interesting insights for future actions in this area.

## Keywords

Cybersecurity, Education, Awareness, Human factors, Digital Citizenship

---

## 1. Introduction

Cybersecurity is a very hot topic for all countries, since cyberattacks continue to increase (SonicWall, 2022), producing negative effects on the general economy (Haislip et al., 2019).

The current approach to cybersecurity tends to consider this issue as an IT problem and consequently to manage it technically, while it is now imperative to go beyond technical skills for creating a future cybersecurity workforce that is really effective (Dawson & Thomson, 2018). In this perspective, given the increasingly digitized world and the growing importance of digital skills, digital citizenship education is central to lead individuals to manage digital technologies effectively (Choi, 2016; Meghan et al., 2019).

It is interesting to observe how the concept of digital citizenship (Future Learn, 2021), consisting of the ability to understand and use digital technologies responsibly, ethically and legally (Council of Europe) has evolved over the last few years. In particular, it has extended its area of influence including various elements, such as communicating online, protecting data, managing cyberbullying, and being aware of the cyber security threats in digital space.

Developing good digital citizens requires appropriate education programs that should be deployed since primary

schools. In fact, considering the wide use of digital technologies by children at a very early age (Hatzigianni & Kalaitzidis, 2018), it is fundamental to educate them on the potential risks they have to face when using communication tools (Rahman et al., 2020). On the other hand, raising awareness of the risks encountered when navigating on the Internet and developing initiatives supporting educators are both important activities foreseen in the Digital Education Action Plan for 2021-2027 (European Commission, 2021).

In the light of what discussed above, developing digital citizenship through awareness actions represents the foundation of cybersecurity education (Corradini & Nardelli, 2020). Moreover, given the age of students in primary school, we think that talking of digital citizenship is more appropriate rather than speaking about cybersecurity, a concept more suitable for businesses and critical infrastructures, calling up attacks and cyber threats. Finally, even though cybersecurity is a fashionable term (Schatz et al., 2017), its use mainly evokes technical aspects, underestimating the human element, whose involvement for managing cybersecurity effectively is crucial (Corradini, 2020; Jeong et al., 2019).

## 2. Methodology

This study investigates the awareness actions deployed by Italian teachers in primary and secondary schools, in accordance with the Italian law n.92 of 20th August 2019 “Introduction of the compulsory civic education”, that includes, among others, the teaching of the subject “Digital Citizenship”.

Developing digital competences and making students aware of the risks of digital technologies are the main goals of Programma il Futuro project (Corradini et al., 2017; Nardelli & Corradini, 2019), whose approach is to integrate the knowledge of the scientific principles of informatics together with the responsible use of digital technologies.

Even though the study of informatics is not mandatory in Italian school system, the project has involved since 2014 more than 60,000 teachers and over 3 million students. In April 2022, Programma il Futuro has been recognized as the best Italian initiative in the area “Digital for Schools” by the Department of the Digital Transformation of the Presidency of Italian Council of Ministers.

Project monitoring is done every year by means of a questionnaire, in order to evaluate teachers and students’ participation, their level of satisfaction, the quality of materials provided. One section of this questionnaire is dedicated to “digital citizenship” to investigate what teachers think of the relationship between their students and digital technologies, and the actions they put in place during the school year. This section, initially consisting of 15 multiple-choice questions and 1 open-ended question, has been expanded during the last monitoring activity with two additional sections, one investigating the use of social media, and the other dedicated to the actions deployed by teachers to be compliant with the Italian law cited above. The current version of the questionnaire includes more than 40 items.

The questionnaire was sent in January 2022, through the project platform. Answers were provided by 1,008 teachers, presenting the following demographic characteristics: Gender (F: 85%; M: 15%); Age (up-to-30: 0,2%; 31-40: 3,7%; 41-50: 28,4%; 51-60: 54,8%; 61-and-up: 13%). The gender distribution is consistent with the national distribution of teachers’ gender.

The majority of teachers is from primary school (58%), then around a quarter (26%) from middle school, and a minority is from high school (11%). Most of them (87.6%) have more than ten years’ experience in teaching. Finally, among the disciplines taught by the sample, the most representative ones are: mathematics (49%), sciences (37%), informatics (32%), followed by Italian (26%) and other humanistic disciplines. This result shows how teachers involved in the project do not belong to technical disciplines only, and this is one of the reasons explaining the large participation of primary schools, as confirmed by the last three years of the project (Corradini & Nardelli, 2021). Moreover, for what regards student participation, the interest towards the project activities is very high for both boys and girls (90%).

In this paper, we present the main results of the section “Digital citizenship” of the questionnaires filled out by teachers, given their direct involvement in teaching civic education. The areas of the questionnaires are described in **Table 1**.

## 3. Results and discussion

In this section we present and discuss the main results of the four areas listed in **Table 1**.

### 3.1 Area 1: Responsible use of digital technologies

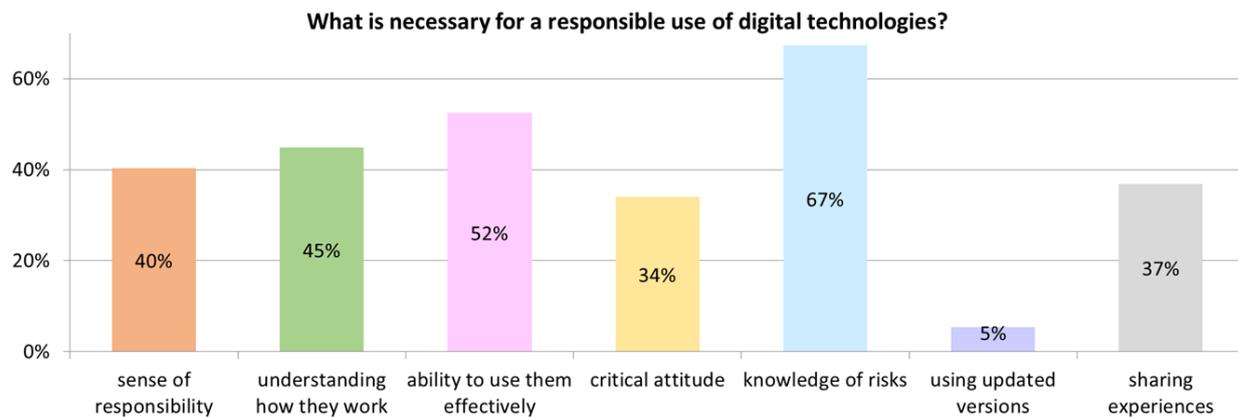
According to teachers, an ‘adequate knowledge of risks associated with their use’ (67%) is the most important element for developing a responsible use of technologies, followed by ‘the ability to use them effectively’ (52%), ‘understanding how they work’ (45%), and ‘sense of responsibility’ (40%), see **Figure 1**. It was possible to select up to 3 answers out of 7. These results confirm the trend emerged from the monitoring activities in previous years (Corradini & Nardelli 2021), so highlighting the importance of the human element and the specific need of implementing awareness

activities to manage risks while using digital technologies.

**Table 1. Areas of the questionnaire “Digital citizenship”**

Nr.	Areas	Description
1	Responsible use of digital technologies	This area investigates teachers’ beliefs about the responsible use of digital technologies and what is needed to help students to develop a conscious use of them.
2	The use of social media and the relative risks	This area explores the use of social media platforms and chatting apps by teachers, and their perception about the exposition to risks for them and for students.
3	Teaching digital civic education and assessment of materials provided by the project	This area investigates how many actions teachers have deployed to promote digital citizenship for their students related to the reliability of sources of data, the use of digital communication tools, the comprehension of the digital context, data protection and digital identity, and so on. Moreover, teachers are asked to evaluate the usefulness of the various guidebooks provided by the project for teaching digital civic education (e.g.: Super Digital Citizen; The Power of Words; Private and Personal Information; Safe Online Talk; Going Places Safely). These guidebooks, translated and adapted from Common Sense materials, are intended for teachers use, and consist of fully developed lesson plans, exercises included, on different digital issues (e.g. using the Internet and social network safely, keeping personal data private and protecting digital reputation). Educational materials are also available for parents.
4	Supporting teachers in digital education	This area explores what types of activity are useful to support teachers in developing a proper digital citizenship among their students (e.g. training, communication). Moreover, teachers express their needs to achieve an adequate preparation for teaching digital citizenship in their classrooms.

Note that the area “Teaching digital civic education” was introduced in the 2022 version of the questionnaire, after the approval of the law 92/2019 “Introduction of the compulsory civic education”.



**Figure 1. Elements for developing a responsible use of digital technologies.**

### 3.2 Area 2: The use of social media and the relative risks

Not only students, but also teachers use social media platforms and chatting apps, essentially for ‘getting in touch with other people’ (84%), ‘being informed about the world’ (65%). As you can see in **Figure 2**, YouTube is the most used social media platform (82%), followed by Facebook (75%) and Instagram (50%), while WhatsApp is the most used chatting app (97%) followed by Messenger (42%) and Telegram (41%). Teachers could select all the ones they use among a large set and we show in the figure only the most used ones.

As a significant result in this area, teachers think that these tools expose both them and students to the risk of addiction: while for themselves the risk of developing ‘addiction’ is 61% (**Figure 3**), teachers’ perception of this same risk for their students grows up to 73% (**Figure 4**). Moreover, while teachers feel personally worried about the ‘spread of fake news’ (56%), they think that the second most relevant risk for their students is represented by online ‘dangerous encounters’ (63%).

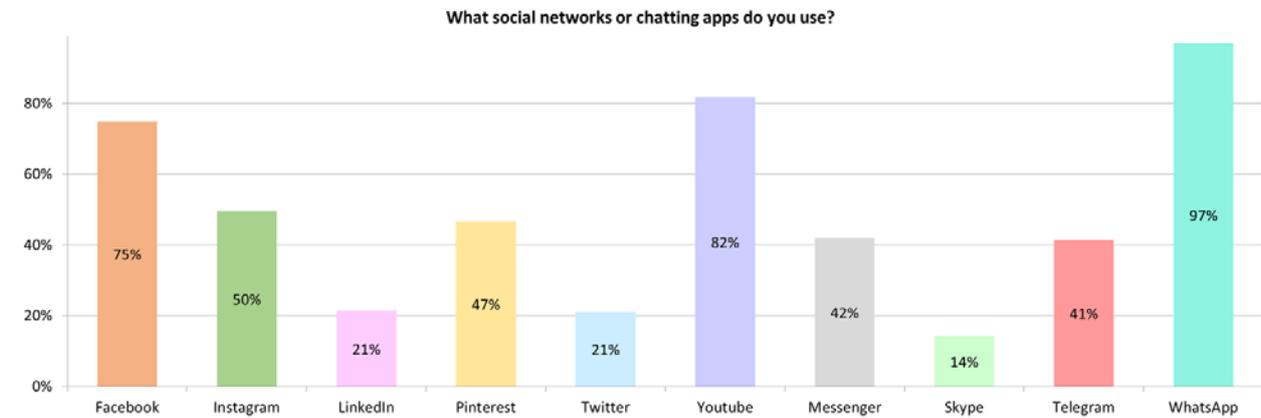


Figure 2. Use of social media platforms and chatting apps by teachers.

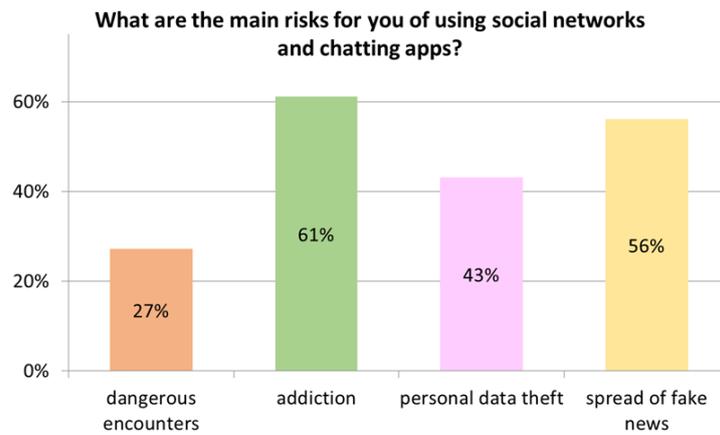


Figure 3. Personal risks derived from the use of social media platforms and chatting apps.

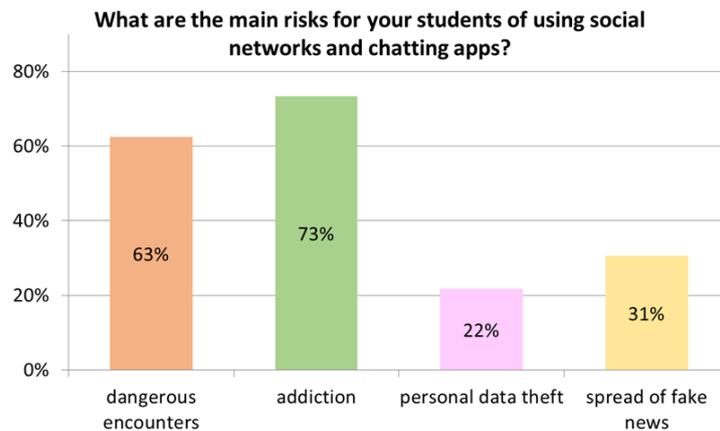


Figure 4. Teachers' perception of the risks derived from the use of social media platforms and chatting apps for students.

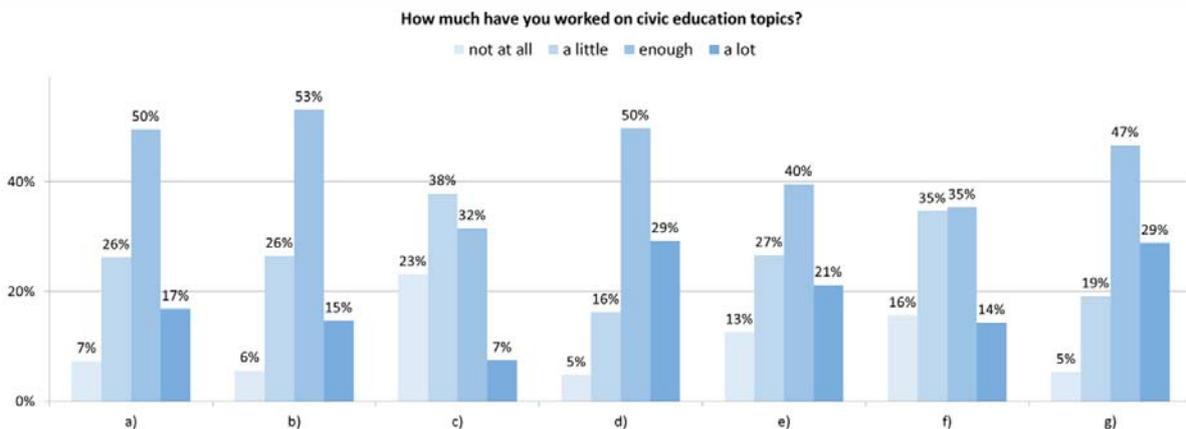
### 3.3 Area 3: Teaching digital civic education

Teachers were asked to evaluate, using a 4-point Likert Scale where 'not at all' is the minimum and 'a lot' the maximum, how much educational activity they deployed for the following topics (that, in synthesis, are the ones identified

by the law 92/2019):

- analyzing, comparing and critically evaluating the credibility and reliability of the sources of data, information and digital content;
- interacting through various digital technologies and identifying the appropriate digital means and forms of communication with respect to a specific context;
- getting informed and participating in the public debate through the use of public and private digital services;
- being aware of the rules to use in the digital context, so adapting communication strategies to specific audiences and considering cultural and generational diversity in digital environments;
- creating and managing digital identity, being able to protect one's own reputation, managing and protecting data produced through various digital tools, environments and services;
- knowing the policies on the protection of confidentiality applied by digital services regarding the use of personal data;
- being able to avoid health risks and threats to one's physical and psychological well-being when using digital technologies, with particular attention to behaviors related to bullying and cyberbullying.

As you can see in **Figure 5**, activities on digital education have been unevenly distributed. The aggregation of the positive values (i.e.: 'enough' and 'a lot') of Likert items shows how teachers essentially worked more on some topics, namely 'the rules to use in the digital context' (79%, topic d) and 'avoid risks and threats to one's own well-being' (76%, topic g). This is easily understandable, given the high attention that this matter has received in school over the years.



**Figure 5. Activities deployed by teachers on digital civic education.**

Moreover, a specific anti-cyberbullying law in Italy (Law 71/2017) has identified several actions that teachers have to undertake to deal with this phenomenon in schools. On the other hand, when teachers were asked which are the highly important topics students have to know to move safely in the digital world, the three most selected ones out of a list of five were: 'online harassment' (82%), 'safe online behavior' (80%) and 'data protection and privacy' (79%) (**Figure 6**).

Some topics, regarding 'the participation in the public debate through the use of public and private digital services' (topic c, where the aggregation of negative values, i.e.: 'not at all' and 'a little', of Likert items reaches a value of 61%), and 'the knowledge of the policies of the protection of confidentiality about personal data' (topic f, where the same aggregation reaches 51%) lags behind in implementation. Maybe, considering the recent adoption of the law and that slightly more than half of teachers belongs to primary school, it is possible to suppose that they decided to concentrate their attention on topics they perceived more relevant and urgent for smaller pupils, delaying to the next year a full implementation of the teaching plan.

Finally, on the qualitative side, the open-ended question has provided interesting insights, since teachers declare to need more materials for developing digital civic education. This qualitative analysis is very important for steering the project towards its future activities (see the results of area 4).

Teacher that used the guidebooks provided by the project and containing lessons for developing digital citizenship confirm their usefulness and the need of receiving updated materials on the various digital issues. Note that guidebooks have been downloaded more than 135.000 times and the videos associated with them have received more than 400.000 views. Teachers who have not yet used these materials declared their intention to apply them in their classrooms shortly.

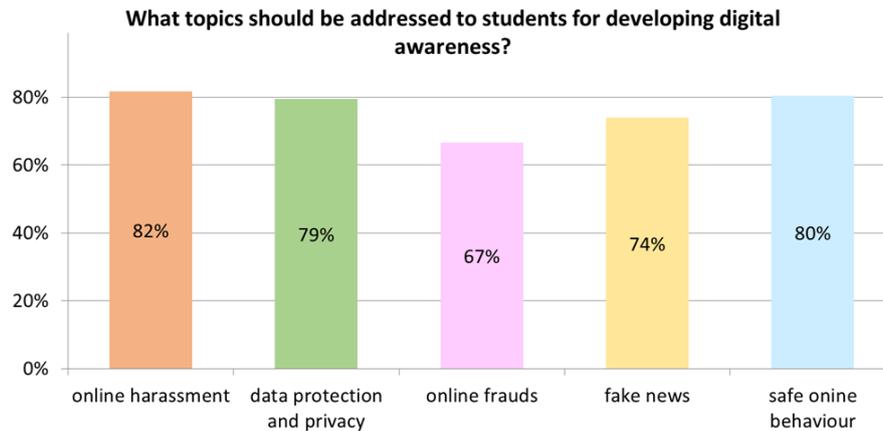


Figure 6. Topics for educating students to move safely in the digital world.

### 3.4 Area 4: Supporting teachers in digital education

Teachers were asked to indicate what actions should be deployed to support them in developing digital citizenship among their students. They could select in a list containing 7 items all the ones they considered important, with the possibility of providing additional suggestions through the item option ‘other’. ‘Sharing experiences’ (66%), ‘parents’ involvement’ (52%) and ‘classroom training’ (43%) were selected as the most important actions to achieve the goal, followed by ‘webinar’ (40%). Note that since 2019 the project has planned webinar on digital and cybersecurity issues addressed to teachers by involving experts on the topics dealt with.

In addition, 97% of teachers are aware that, considering the wide use of digital technologies, they need to receive an ad-hoc training. By selecting up to 4 answers out of 7, they indicated that the most important topics that should be part of their specific training are ‘social media use’ (68%) and ‘recognizing fake news’ (60%), while ‘online harassment’ and ‘identity theft’ are perceived equally relevant (50%) (Figure 7).

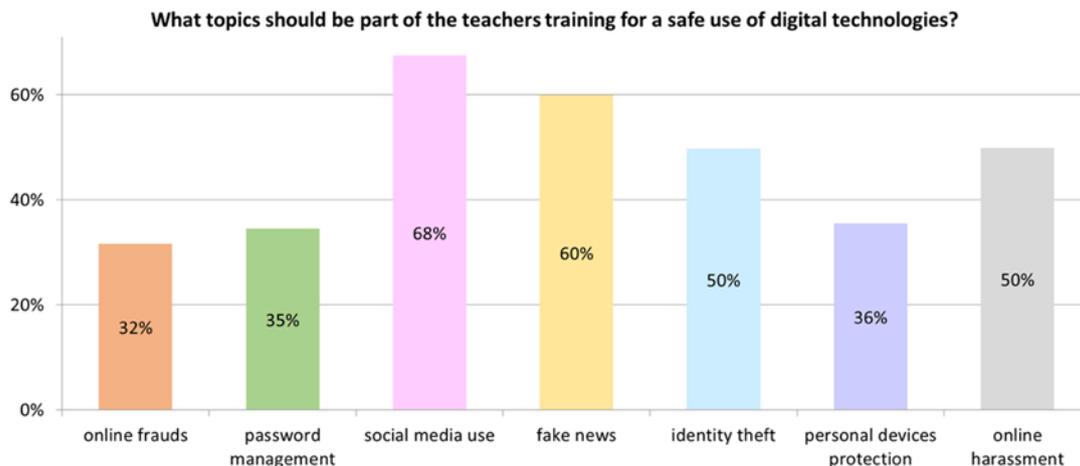


Figure 7. Topics for teachers training.

## 4. Conclusions

In this paper, we have discussed the digital awareness actions deployed by Italian teachers in primary and secondary schools, involved in Programma il Futuro project.

It is clear that education is the main road to prepare future citizens able to use digital technology responsibly, ethically and legally. This approach should be considered the foundation of cybersecurity education, given that teaching digital citizenship means dealing with various connected elements, such as communicating online, protecting data and digital identity, moving safely on the Internet, and being aware of cyber security threats. Investing in digital civic education is

therefore the best action to face the challenges posed by the digital society, cybersecurity threats included.

To achieve this goal, teachers need to be prepared and supported, also providing them adequate and updated educational materials for their students. This is what Programma il Futuro project has developed since 2014, involving teachers, students and parents in the various activities, and combining the actions of spreading the scientific principles of informatics and sensitizing students towards a responsible use of digital technologies. For these purposes, it provides lessons based on materials created by Code.org and Common Sense, two important international no profit organizations specialized on educational activities.

Answers from 1,008 teachers - belonging to primary and secondary school - confirmed their need to be assisted in managing students' preparation on digital citizenship, also to be compliant with the Italian law n.92 of 20th August 2019 'Introduction of the compulsory civic education'. This is certainly an excellent driver to actively involve teachers and students in a digital education plan.

Going beyond cyberbullying, digital civic education enlarges the horizon of the items to be discussed with students in order to prepare them to participate in the public debate in an increasingly digital society.

Finally, further considerations should concern the use of the term cybersecurity in school context. This term is certainly fashionable, but given the age of students in primary school, teaching digital citizenship appears more appropriate rather than teaching cybersecurity. The concept, in fact, is more suitable for businesses and critical infrastructures, but excessive for kindergarten.

Various actions will be planned within the project for the next years to come, and the continuous monitoring activity will help to identify the best initiatives to spread out.

## Acknowledgements

We thank all teachers involved in "Programma il Futuro" for their continued participation to the project and their involvement into this research. Thanks also to Common Sense for having provided us the digital citizenship teaching material and to Code.org for their activity to support Informatics education in schools. We are also grateful to project's sponsors: Eni, Engineering, Seeweb; for their support.

## References

- Choi, M. (2016). A Concept Analysis of Digital Citizenship for Democratic Citizenship Education in the Internet Age. *Theory & Research in Social Education*, 44:4, 565-607.
- Corradini, I. (2020). *Building a Cybersecurity Culture in Organizations. How to bridge the gap between people and digital technology*, Springer (2020).
- Corradini, I., Lodi, M., Nardelli, E. (2017). Conceptions and Misconceptions about Computational Thinking among Italian Primary School Teachers. In 13th ACM Annual Conference on International Computing Education Research (ICER-2017), pages 136-144, Tacoma, WA, USA, August 2017.
- Corradini, I., Nardelli, E. (2020). Developing Digital Awareness at School: A Fundamental Step for Cybersecurity Education. In I. Corradini, E. Nardelli, T. Ahram (eds), *Advances in Human Factors in Cybersecurity*. AHFE 2020. Advances in Intelligent Systems and Computing, vol 1219. Springer.
- Corradini, I., Nardelli, E. (2021). Promoting digital awareness at school: a three-year investigation in primary and secondary school teachers. In 13th International Conference on Education and New Learning Technologies, Online Conference. 6-7 July, 2021. (EDULEARN 2021), pages 10443-10447.
- Council of Europe, *Digital Citizenship and Digital Citizenship Education*, <https://www.coe.int/en/web/digital-citizenship-education>.
- Dawson, J., and Thomson, R. (2018). The Future Cybersecurity Workforce: Going Beyond Technical Skills for Successful Cyber Performance". *Frontiers in Psychology*, 9, 744.
- European Commission. Digital education action plan 2021-2027 (2021). [https://education.ec.europa.eu/education-in-the-eu/digital-education-action-plan\\_en](https://education.ec.europa.eu/education-in-the-eu/digital-education-action-plan_en).
- FutureLearn (2021). *What is digital citizenship? – A guide for teachers*. September 2021. <https://www.futurelearn.com/info/blog/what-is-digital-citizenship-teacher-guide>.
- Haislip, J., Kolven, K., Pinsker, R., Steffen, T. (2019). *The Economic Cost of Cybersecurity Breaches: A Broad-Based Analysis*. The 2019 Workshop on the Economics of Information Security.
- Hatzigianni, M., & Kalaitzidis, I. (2018). Early childhood educators' attitudes and beliefs around the use of touchscreen technologies by children under three years of age. *British Journal of Educational Technology*, 49(5), 883-895.
- Jeong, J., Mihelcic, J., Oliver, G, Rudolph C (2019). Towards an improved understanding of human factors in cybersecurity. In 2019

IEEE 5th *International Conference on Collaboration and Internet Computing (CIC)* Dec 12 (pp. 338-345).

Nardelli, E., Corradini, I. (2019). Informatics Education in School: A Multi-Year Large-Scale Study on Female Participation and Teachers' Beliefs. In *12th International Conference on Informatics in Schools: Situation, Evolution, and Perspectives (ISSEP-2019)*, pages 53-67, Larnaca, Cipro, November.

Rahman, N. A. A, Sairi, I. H., Zizi, N. A. M., and Khalid F. (2020). The importance of cybersecurity Education in School. *International Journal of Information and Education Technology*, Vol. 10, No. 5.

Schatz, D., Bashroush, R., and Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law*: Vol. 12: No. 2, Article 8.

SonicWall. (2022). *Cyber threat Report* <https://www.sonicwall.com/2022-cyber-threat-report/>.

Walters, M., Donna, G., and Shereeza, M. (2019). *A Literature Review-Digital Citizenship and Elementary Education*. Walden Faculty and Staff Publications. 309.