RESEARCH ARTICLE WWW.PEGEGOG.NET

Selected Risks of Cyberspace in the Transition of Pupils to Distance Learning in Czech Republic

Helena Mičková[1*], Jana Miková[2], Zdenka Nováková[3], Jan Šmída[4]
[1-4]Palacky University, Žižkovo nám. 5, Olomouc 77900, Czech Republic

Abstract

The development of communication and information means, especially the presence of the online environment, is undoubtedly an integral part of pupils' leisure time. During the pandemic, it also inevitably became a standard part of formal education in the form of so-called distance learning. On 11 March 2020, an extraordinary measure of the Ministry of Health entered into force, resulting in the widespread closing of schools. The extraordinary measure was later replaced by the Resolution of the Government of the Czech Republic No. 74/2020 Coll. of 12 March 2020. On 12 March 2020, a state emergency was declared.

The main research goal is to name selected related cyberspace risks with the transition to distance learning and their potential intensity, which threatened or may continue to threaten students in the transition to this model of education. Research sub-objectives are to analyze students' awareness of their rights and obligations in the context of cyber security in distance learning and to compare the obtained data among primary and secondary school pupils.

Research and achievement of set research goals are carried out through a quantitative and qualitative approach through piloting in the form of interviews with a selected sample of students, and the use of a questionnaire survey focused on the occurrence of selected risks in cyberspace and finding out essential awareness of students' rights and obligations in cyber security.

Keywords: Education, cyberspace, pupils, digital technologie

Introduction

In response to the Covid-19 pandemic in mid-March 2020, traditional teaching moved to a digital environment. The Ministry of Education, Youth and Sports of the Czech Republic issued the Methodological Recommendation for Distance Education (2020). The School Act then legislatively established a new method of distance education, providing the obligation of distance education in extraordinary situations during which pupils cannot participate in faceto-face teaching. At the same time, the obligation of pupils to be educated in this way was established (Zákon č. 561/2004 Sb.). School management and teachers had to adapt to the new situation. They had to offer students possible means of distance education and find the most diverse online teaching methods.

There are many definitions for distance education. According to Průcha and Míka (2000), distance education is any form of education in which the individual student is not under the constant supervision of a teacher but has a curriculum at his disposal, consultations are available, and is distantly guided by the teacher (cf. Všetulová et al., 2007). Černý (2015, p. 34) defines distance education as a form of education in which students are in indirect contact with the teacher, education is primarily self-directed, and the student bears tremendous responsibility for the results and the process of education.

According to Zlámalová (2007, p. 30), distance education aims to make education accessible to all those who are not, or cannot be, present otherwise. In the provided definitions, we uncover certain features common to the distance form of education, namely distance education in the form of space or time, the use of modern technologies, and pupils' independence. Other characteristics of distance education include time and content flexibility, the necessary independence of pupils, and individualization during teaching.

Through the Methodological Recommendation of the Ministry of Education, Youth and Sports (Ministry of Education, Sports and Education, 2020a), distance education can be implemented through online or offline teaching. We understand online teaching as teaching carried out via the Internet, digital technologies, and software tools. In synchronous online teaching, students are present with the teacher in real-time and place, whereas in asynchronous teaching, students work independently on assigned tasks, taking into account their learning pace and other conditions. Offline learning does not occur via the Internet but includes selfstudy and completing assigned tasks in written or another form.

One of the characteristics of distance education is also the possibility of using various information and communication technologies, but at the same time, this form of education brings problems of insufficient motivation and inexperience

Corresponding Author e-mail: jan.smida02@upol.cz

How to cite this article: Mičková, H Miková J, Nováková Z, Šmída J. Selected Risks of Cyberspace in the Transition of Pupils to Distance Learning in Czech Republic. Pegem Journal of Education and Instruction, Vol. 13, No. 4, 2023, 323-329.

Source of support: None

Conflict of interest: Nil.

DOI: 10.47750/pegegog.13.04.37

Received: 19.12.2022

Accepted: 02.02.2023 **Publication:** 01.10.2023

with modern technologies and distance education in general (Zlámalová, 2007; Bednaříková, 2013). Gluoksnyte & White (2022) also mentions difficulties with equipment, lack of opportunities for students to engage in social and community activities communication skills and the difficulty of securing the required exam (Gluoksnyte & White, 2022).

The Czech School Inspectorate (CSI), which conducted controlled telephone interviews with principals of primary and secondary schools from April 1 to 14, 2020, found out that the most common communication platforms between teachers and pupils were the following: WhatsApp, the information system Bakaláři (in high schools), they also communicated frequently via email or social networks. In the annual report for the 2020/2021 school year, the Czech School Inspectorate reflects the positive aspects of the methodological recommendation of the Ministry of Education, Youth and Sports to use a unified communication platform and, in particular, a video conference system for synchronous and asynchronous distance education (Annual report of the Czech School Inspectorate, 2021). Compared to the closing of Czech schools in the spring of 2020, the video conference systems Microsoft Teams and Google Meet (Google Classroom and Google Workspace) were primarily used. At the same time, the Czech School Inspectorate appealed for proper prevention in the field of cyber security and data protection in cyberspace, considering the amount of time spent on tablets, computers, and the Internet.

The transition to online education has grown by leaps and bounds precisely due to the covid pandemic. To ensure distance learning, schools and teachers could fail to respect the age limit of some communication applications and thus violate the law on processing personal data. The law states that children acquire the capacity to grant consent to the processing of personal data in connection with the offer of information society services directly to them upon reaching the age of fifteen (Act No. 110/2019, Coll.).The WhatsApp application, which, according to an investigation by the Czech School Inspectorate (2020), was used most often by schools, teachers, and pupils during the closing of schools, however, had an age limit of 16 years but was often used by younger children. Another problem with distance education was taking and sharing recordings (including snapshots and screenshots) from video conferences on social networks or school websites (Kopecký, 2020).

The situation in education during the Covid-19 pandemic tested everyone's knowledge of digital and communication tools. It pointed out the positives and negatives of distance education and provided an insight into the possibility of its future use. At one point, without any preparation, it was necessary to switch to online education. During the first days of distance learning, everyone tried to adapt to the situation according to their abilities, and there was no time to think about the possible risks of the online environment. Education suffered from students' and some teachers' poor digital literacy (Bergdahl & Nouri, 2021). Studies show that this topic needs to be addressed more effectively and should not be underestimated with which also agree (Metin Karaaslan et al., 2022).

The various dangers of cyberspace might affect many areas of human life. Addictive behavior (Peris et al., 2020) or a threat to privacy in connection with sending intimate photos (Paluckaitė & Žardeckaitė-matulaitienė, 2021) may arise. Another widespread phenomenon related to frequent Internet use is cyberbullying (Hoareau et al., 2021). Cyberstalking is frequent and involves even teachers (Cohen-almagor et al., 2022). In this way, it would be possible to name several other phenomena in the context of social networks and the Internet in general. However, what they have in common is any privacy violation and unauthorized handling of personal data, which can lead to many legal consequences (Johnson et al., 2019).

On March 11, 2020, an extraordinary measure of the Ministry of Health entered into force, resulting in the widespread closure of schools (Extraordinary measures of the Ministry of Health 10676/2020-1/MIN/KAN). The extraordinary measure was later replaced by Resolution of the Government of the Czech Republic No. 74/2020 Coll. dated 12/03/2020. The given resolution has ceased to be effective as of the current date. A state of emergency was also declared on the territory of the Czech Republic on March 12, 2020 (Resolution of the Government of the Czech Republic of March 12, 2020, No. 194). Schools were obliged to continue to provide teaching, but in a non-contact manner, preventing the personal participation of pupils in teaching. The schools thus found themselves in a completely new situation, which had to be dealt with by the management as well as the teachers and students. In cooperation with the Ministry of Health, the Ministry of Education, Youth, and Sports issued manuals for individual types of schools, talking about which measures must be followed by individual workers and pupils of these schools (Ministry of Education, Sports and Culture, 2020). As a result of the development of the situation and long-term outages in the contact form of teaching, there was also a change in legislation, specifically to an amendment to the Education Act, which, in the provisions of § 184, paragraph a, enshrined the obligation to teach distantly, with distant education being understood as non-contact teaching using ICT (information and communication technologies).

The Covid-19 pandemic has forced teachers worldwide to switch to distance learning. During this period, new situations began to arise in the online environment related to the violation of privacy and protection of personal data in connection with this new type of education. Articles in the media also drew attention to this situation within the Czech Republic. Those focused, for example, on the inappropriate names of pupils' e-mails. The first and last name in the title of the e-mail is completely inappropriate for students, and they can be identified quite easily. Applications chosen in the first stages of distance education can be considered problematic. For example, teachers used platforms run by the company Meta, such as WhatsApp or Messenger. However, no one mainly thought about the fact that the company does not allow children under the age of 13 to use its services. There was also a problem with setting teacher and student roles in selected applications or weak and simple passwords used to access online classes. Furthermore, there was the taking of teaching records, which were later leaked outside the secure environment of the school, and several other risky phenomena (Kopecký, 2020).The annual report of the Czech School Inspectorate (CSI) focused on the quality and effectiveness of education and the educational system in the 2020/2021 school year brings several exciting findings in the field of distance education. It is possible to perceive the fundamental shift of teachers in the field of digital technologies as positive. However, there was a difference between the schools, where teachers felt insufficient support from the school management during distance education and the availability of professional help with digital technologies. This is related to the findings that in about 1/3 of the cases, teaching was disrupted by technical problems. The CSI came to unexpected results when examining pupils' awareness of the recording of lessons. Only 1% of first-grade pupils were informed that a video recording of the lesson was being taken. In the case of second-grade pupils, this was 2% of them. The CSI also mentions that there have been several cases where sensitive or personal data was made public and shared content was leaked to the public network. At the end of the report, it was stated, among other things, that compliance with the rules of cyber security failed to a certain extent during distance education (Annual Report of Czech School Inspectorate, 2021). Parents have an even more critical role than the school. Their behavior on social networks forms the child's digital identity since birth. It is crucial to approach this topic responsibly and with a certain amount of knowledge of social network risks and personal data protection. With older children, parents often do not even know what the children share about themselves on the Internet, and with younger children, the parents themselves share large amounts of data (Aswathy Prakash, 2019). These conclusions are also agreed by (Riesmeyer et al., 2019), who studied several dozen families in depth. They found that parents are often more protective of their privacy and personal data than of their children's data. In connection with the protection of personal data, the General Data Protection Regulation (GDPR) entered into force on May 25, 2018, within the European Union (EU) framework. This regulation replaces Act No. 101/2000 Coll in the Czech Republic. On the protection of personal data (Orientation in GDPR, 2022). Among other things, the regulation refers to the "right to erasure," which should, given the applicable exceptions, enable the erasure of the child's personal data. However, how this will be realistically dealt with in the future is not yet completely clear; only time will show. Here again, the question arises of the level of digital literacy and awareness of this regulation, both among parents and children. However, the main concern should be protecting the children's rights and their right to privacy (Lievens &

Maelen, 2019). Parents should realize that, by sharing various information, they create a digital footprint for their children, which can impact their future personal and professional life (Brosch, 2018). Children are often unaware of the consequences of their actions. Some of the digital literacy concepts are too abstract for them, and they cannot adequately evaluate the situation (Brooks & Moeller, 2019).

Methodology

For our research purposes, we used a quantitative research strategy; as a research tool, a classic questionnaire survey was used. Questionnaire surveys are among the most widespread forms of data collection. For our research purposes, the data was subsequently analyzed using statistical methods.

The research group consisted of students in the second grade of primary schools, secondary schools, high schools, conservatories, and other schools that fall within the 2nd to 3rd level of education classification according to ISCED. A total of 315 respondents participated in the survey, of which 210 were women, and 84 were men. The other respondents either did not want to state their gender or identified themselves as different.

The age distribution of the pupils is between 16 and 19 years old, so it was mainly high school pupils.

Results

The main research goal was to name selected related cyberspace risks with the transition to distance learning and total number of respondents was 315.

The graph 1 describes how students communicated with their friends during distance learning. The most common is communication through chatting (via such applications

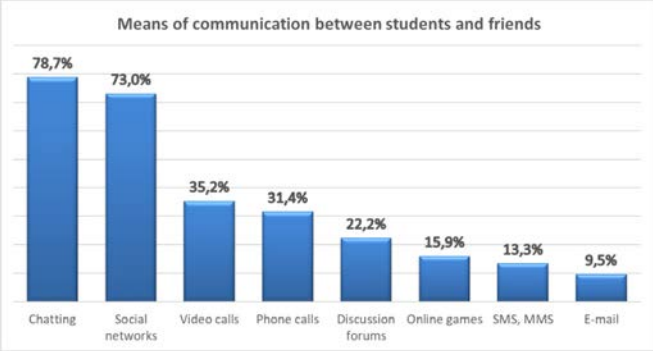

Chart 1: Means of communication between students and friends.

as Messenger, Viber, and WhatsApp) and social networks (via such applications as Facebook and Instagram), used by approximately three-quarters of the pupils. Approximately one-third of the pupils used video or telephone calls.

To connect to classes, pupils usually used laptops (71.5%) and mobile phones (66.5%); see the chart 2.

The questionnaire survey revealed that 69,9% of students created an account on the online learning platform themselves. It was confirmed that no elementary school students created an account on the platform alone, which follows up on the findings from graph 4. It clearly shows that only 21,6% of pupils correctly state from what age they can use communication platforms.

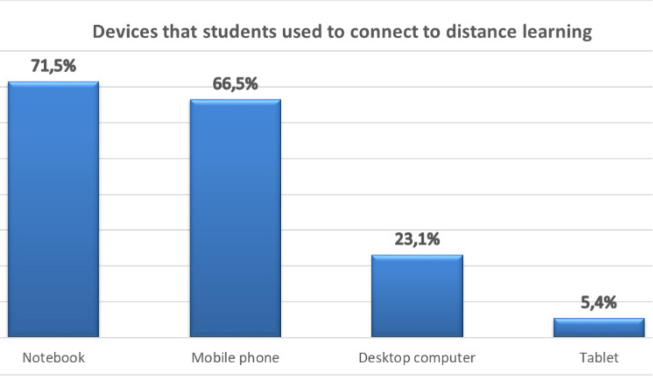

Chart 2: Devices that students used to connect to distance learnig.

As stated in chart No. 1, 73% of pupils used social networks to communicate with their friends during the distance learning period, yet 65,7% do not know or incorrectly state the age limit necessary to meet the conditions of use. The most significant risks of using social networks at a young age arise mainly from the inability to distinguish between truth and reality.

Let us now take a closer look at the issues of cyberattacks, risky behavior, and risky situations in cyberspace, which directly threatened pupils. First, let us look at chart No. 5, which compares the occurrence of given risky situations and cyber-attacks.

It is alarming that 15.2% of students experienced mockery due to a video recording of their person, and 14% of students experienced mockery due to a photo of their person at least once during online teaching. This could undoubtedly have an impact on mental health and social ties. Even more worrying is the finding that 9.2% of pupils experienced threats (and 9.5% even blackmailing) during distance learning. 17.1% of

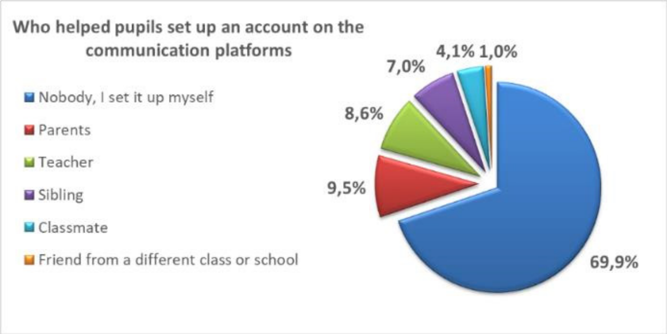

Chart 3: People, who helped pupils set up an account on the communication platforms.

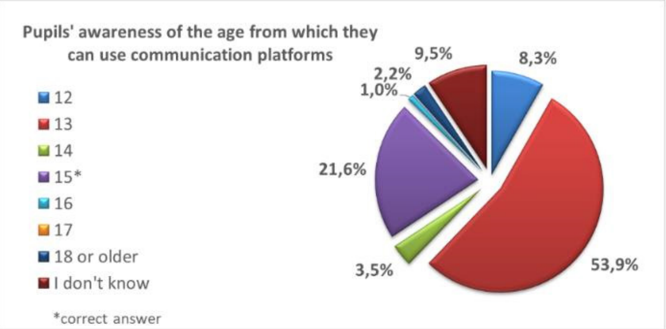

Chart 4: Pupils´awereness of the age from which they can use communication platforms.

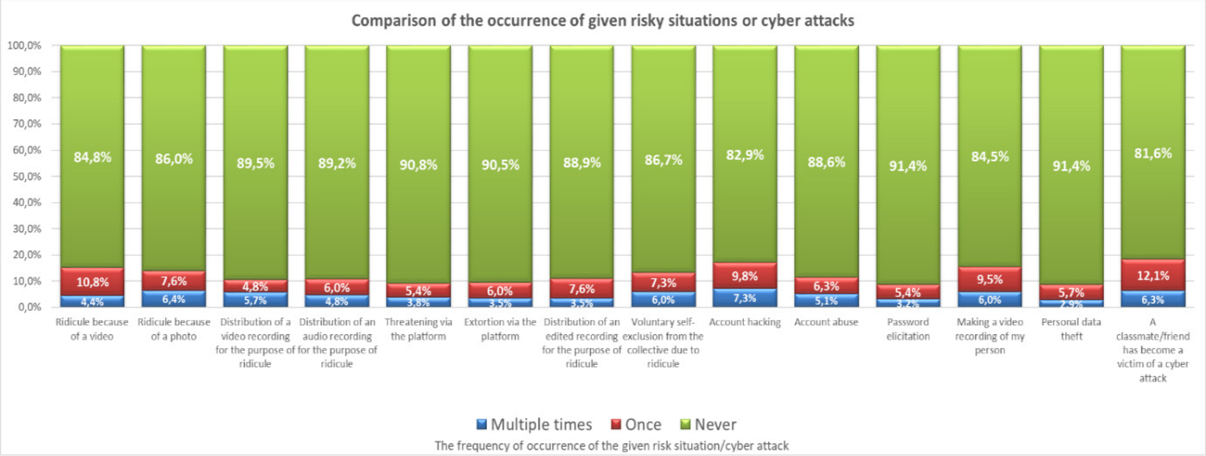

Chart 5: Comparison of the occurrence of given risky situations or cyber attacks.

pupils experienced hacking into an account, and 8.6% of pupils experienced personal data theft. Account misuse by another person happened to 11.4% of pupils. 13.7% of pupils voluntarily preferred to separate themselves from the collective due to bullying.

The perpetrators of cyberattacks from the point of view of "pupils-victims" can be seen in chart 6. It turns out that 8.3% of pupils (every 12th child) experienced a cyberattack from a classmate. Other attackers were former friends, strangers, or peers from the same school.

Attacks by teachers, experienced by 1.9% of pupils, are also worth mentioning.

However, our respondents also acknowledge inappropriate behavior distinguished as a cyberattack. 17.8% said they deliberately turned off the teacher's webcam during an online lesson, 16.9% intentionally disrupted the lesson because they were not prepared, and 16.2% disconnected the teacher from the lesson. The finding that a complete 8.9% of pupils intentionally spread a mocking photo or video of a teacher is also severe.

Undoubtedly, students were exposed to cyber risks daily during distance and online learning. 6 The question remains, however, to what extent they were prepared for the transition to such 7 a dangerous environment. The following chart No. 8, reflecting the preventive instruction of 8 pupils regarding possible risks in cyberspace, could help us answer this.

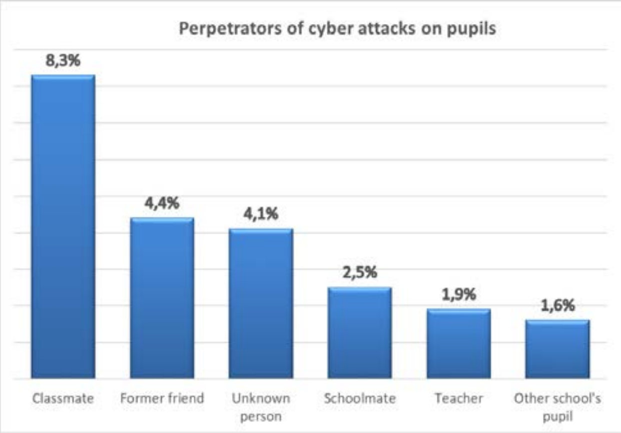

Chart 6: Perpetrators of cyber attacks on pupils.

Chart No. 8 reveals that 41.9% of pupils did not receive any instruction about proper behavior in cyberspace or using communication platforms or social networks. This indeed increased the chance of succumbing to cyber-attacks of all kinds. According to the findings, the school programs and teachers' activities were the main factors in the field of prevention. At the same time, parents played an essential role in this issue for almost a quarter of the pupils.

Based on the collected data, it can be stated with certainty that the preparation of pupils for distance education is insufficient. We can ultimately confirm this using the following findings:

- 70% of pupils created an account on communication platforms by themselves;
- 78% of pupils do not know the age limit for using communication platforms;
- 66% of pupils do not know the age limit for using social networks;
- 41.9% of pupils did not receive instructions about using communication platforms, social networks, and the principles of safe behavior in cyberspace during distance education.

Discussion

As Kopecký (2020) states, one of the problems of distance education is the taking and sharing recordings from video conferences, which also results from our research and is in line with earlier findings in previous researches. According to the individual research items, cyberbullying is also very widespread, which Hoareau et al. (2021) mention in their work. Chart No. 3 and Chart No. 8 also confirm the study by Bergdahl and Nouri (2021), which ensures, in line with our

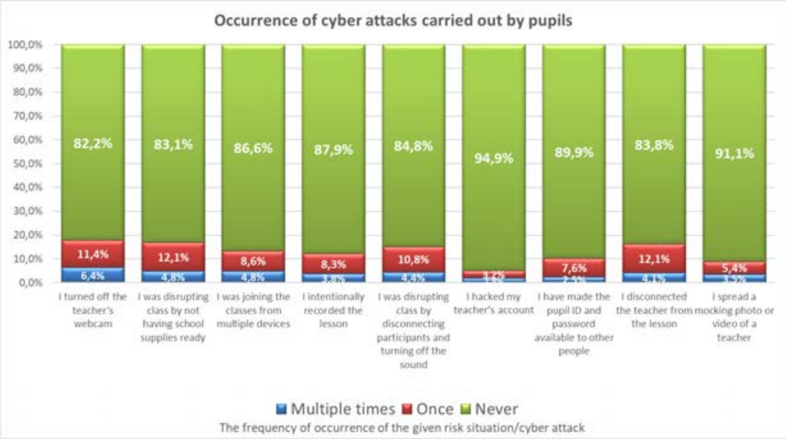

Chart 7: Occurrence of cyber attacks carried out by pupils.

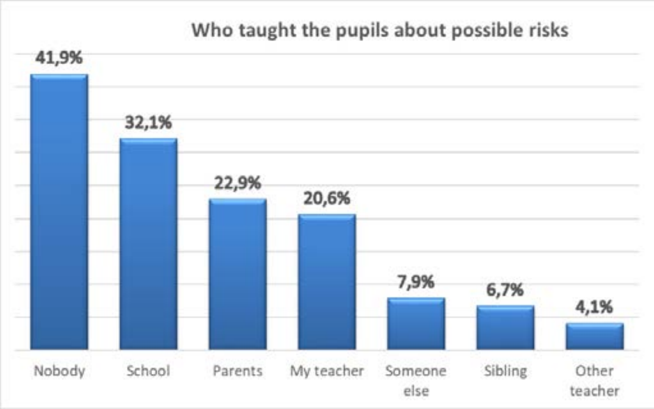

Chart 8: People, who taught the pupils about possible risks.

research, the digital unpreparedness of teachers and students which was more than obvious during the transition to distance learning. In its findings, Ipekli & Titrek (2022) states that teachers' unpreparedness for distance learning is also related to their age and length of practice. Younger teachers prefer to use modern technologies in education more.

If we compare the analyzed data with ongoing research from previous years, we can see constantly increasing numbers in the area of blackmail and threats to children. Ridicule has long been one of the most widespread forms of cyberbullying, which is also confirmed by the obtained data pointing to the fact that roughly every sixth pupil was ridiculed based on the video recording of themselves during online lessons.

We consider the insufficient preventive preparation of pupils for online teaching during distance education the significant finding. In the same way, it is necessary to point out the still high incidence of risky behavior of pupils in cyberspace and the risks, both more and less severe, for which they are not prepared.

Our research shows that a relatively large percentage of adolescents behaved inappropriately towards a teacher in some way, and they themselves referred to this behavior as a cyberattack. Gohal et al. (2023) follow up on these findings with confirmed research results that adolescents who have been victims but have themselves been perpetrators often continue to behave similarly into adulthood. This could be related to our other findings (Mičková et al., 2022) that those who bullied themselves were themselves much more likely to become victims of bullying, but also those who were bullied had a more frequent tendency to take revenge for bullying on their person.

It should also be pointed out that only 22.9% of pupils were instructed by parents and 20.6% by teachers about safe behavior on the Internet. 41.9% were not instructed at all. Only 9.5% of parents and 8.6% of teachers helped pupils set up their accounts. Zhu et al. (2021) report that the influence of parents and teachers plays a pivotal role in preventing and preparing pupils for cyberspace and safe behavior in it. The question remains, therefore, how the percentage distribution of committed and experienced cyberattacks would change if the role of teachers and parents in preparing pupils for the transition to a distance model of education were strengthened.

Findings

For the successful implementation and provision of distance learning, it is, therefore, necessary to always keep in mind the safety of working in the online environment. The school, the parents, and the students' caution should play their role here, based on getting acquainted with the possible risky forms of behavior they may encounter.

We can also speak of significant methodological support for the innovation of informatics in connection with the currently discussed revisions of the framework educational program for primary education in the field of ICT, as well as for the introduction and use of digital technologies in education in general. Of course, these changes also include the building of digital infrastructure in schools and the continuous training of teaching staff. The changes, therefore, aim to strengthen the digital literacy and competencies of those involved in education.

Acknowledgements

The study is part of the following research project – internal grant of Palacký University in Olomouc IGA_PdF_2022_023 named Selected risks of cyberspace in the transition of pupils to distance learnning.

References

Act No. 561/2004 Coll., on preschool, elementary, secondary, higher vocational and other education (Education Act). Online [retrieved 2022-06-30] from: https://www.zakonyprolidi.cz/cs/2004-561

Act No. 110/2019 Coll. Personal Data Processing Act (2019). Retrieved June 29, 2022, https://www.zakonyprolidi.cz/cs/2019-110

Annual report of the Czech School Inspectorate: Quality and effectiveness of education and the educational system in schools in the academic year 2020/2021. (2021). Česká školní inspekce. Retrieved 2022-06-14, from https://www.csicr.cz/CSICR/media/ Elektronickepublikace/2021/Vyrocni_zprava_Ceske_skolni_inspekce_2020_2021/html5/index.html ? pn=1

Aswathy Prakash, G. (2019). Parental role in creation and preservation of digital identity of children. *Test Engineering and Management*, *81*(11-12), 4907 - 4911. https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,shib&db=edselc& AN=edselc.2-52.0-85078356400&lang=cs&site=eds-live&scope=site&authtype=shib &custid=s7108593

Bednaříková, I. (2013). Possibilities and limits of e-learning in secondary education. *EPedagogium*, *2013*(3), 119-128. https://doi.org/DOI: 10.5507/epd.2013.036

Bergdahl, N., & Nouri, J. (2021). Covid-19 and Crisis-Prompted Distance Education in Sweden.

Technology, Knowledge and Learning, *26*(3), 443-459. https://doi.org/10.1007/s10758020-09470-6

Brooks, E., & Moeller, A. (2019). Children's Perceptions and Concerns of Online Privacy.

Extended Abstracts of the Annual Symposium on Computer-Human Interaction in Play

Companion Extended Abstracts, (6), 357-362. https://search.ebscohost.com/ login.aspx?direct=true&AuthType=ip,shib&db=edsair&AN=edsair.doi.dedup.....398828 d77a440b49c7b7cd8057864830&lang=cs&site=eds-live&scope=site&authtype=shib&custid=s7108593

Brosch, A. (2018). Sharenting – Why do parents violate their children's privacy?. *New Educational Review*, *54*(4), 75 - 85. https://doi.org/10.15804/tner.2018.54.4.06

Cohen-almagor, R., Trottier, D., Kacprzyk, J., Gomide, F., Kaynak, O., Liu, D., Pedrycz, W., Polycarpou, M., Rudas, I., Wang, J., & Arai, K. (2022). Internet Crime Enabling: Stalking and Cyberstalking. *Advances in Information and Communication: Proceedings of the*

2022 Future of Information and Communication Conference (FICC), Volume 2, *439*, 843-

859. https://doi.org/10.1007/978-3-030-98015-3_57

Černý, M. (2015). *Distance education for teachers* (2015 ed.). Flow.

Extraordinary measures of the Ministry of Health 10676/2020-1/MIN/KAN (2020). Online
[retrieved 2022-06-30] from: https://www.mzcr.cz/wp

Gluoksnyte, O., White, C., (2022). Distance Learning: Methods and Factors for Effective delivery of Educational Experience. International Journal on Lifelong Education and Leadership, 8, 1-21. https://dergipark.org.tr/tr/pub/ijlel/issue/70779/1096265

Gohal, G., Alqassim, A., Eltyeb, E., Rayyani, A., Hakami, B., Al Faqih, A., ... & Mahfouz, M. (2023). Prevalence and related risks of cyberbullying and its effects on adolescent. BMC psychiatry, 23(1), 1-10.

Hoareau, N., Bagès, C., & Guerrien, A. (2021). Cyberbullying, Self-control, Information, and Electronic Communication Technologies: Do Adolescents Know How to Exercise Selfcontrol on the Internet?. *International Journal of Bullying Prevention: An official publication of the International Bullying Prevention Association*, 1-11. https://doi.org/10.1007/s42380-021-00099-2

Ipekli, N., Titrek, O., (2022). Öğretmenlerin Covid-19 Pandemisi Öncesi ve Sonrasındaki Uzaktan Eğitime Yönelik Tutumlarının İncelenmesi (Sakarya İli Örneği). *Sakarya Üniversitesi Eğitim Fakültesi Dergisi*. 22(2), 29-49. https://dergipark.org.tr/tr/download/article-file/2027984

Johnson, N., Johnson, D., Tweed, P., & Smolla, R. (2019). Defamation and Invasion of Privacy in the Internet Age. *Southwestern Journal of International Law*, *25*(1), 9-41. https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,shib&db=edshol& AN=edshol.hein.journals.sjlta25.5&authtype=shib&lang=cs&site=edslive&scope=site&authtype=shib&custid=s7108593

Kopecký, K. (2020). How to secure online learning. E-Safety. In K. Kopecký, *How to secure online learning. E-Safety* (Vol. 5, pp. 32-39). Univerzita Palackého v Olomouci.

Lievens, E., & Maelen, C. (2019). A Child's Right to be Forgotten: Letting Go of the Past and Embracing the Future? *Latin American Law Review*, (2), 61-79. https://doi.org/10.29263/lar02.2019.03

Ministry of Education and Culture of the Czech Republic: Methodological recommendations for distance education. Edu.cz. Retrieved June 29, 2022, from

https://www.edu.cz/methodology/metodika-pro-vzdelavani-distancnim-zpusobem/

Metin Karaaslan, M., Çelik, İ., Kurt, Ş., Yılmaz Yavuz, A., & Bektaş, M. (2022). Undergraduate nursing students' experiences of distance education during the COVID-19 pandemic.

Journal of Professional Nursing, *38*, 74-82. https://doi.org/10.1016/j.profnurs.2021.11.010

Mičková, H., Miková, J., Nováková, Z., & Šmída, J. (2022). Cyberbullyıng as one of the possıble rısks of dıstance learnıng. In ICERI2022 Proceedings (pp. 3138-3143). IATED. https://doi.org/10.21125/iceri.2022.0785

Methodological recommendations for distance education, Ministry of Education, Culture and Sports (2020) Online [retrieved 2022-06-30] from: file:///C:/Users/uzivatel/Downloads/metodika_DZV__23_09_final%20(2).pd

Orientation in GDPR: What is GDPR. (2022). Ministry of the Interior of the Czech Republic.. Retrieved 2022-06-19, from https://www.mvcr.cz/gdpr/clanek/co-je-gdpr.aspx

Paluckaitė, U., & Žardeckaitė-matulaitienė, K. (2021). Adolescents' intention and willingness to engage in risky photo disclosure on social networking sites: Testing the prototype willingness model. *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, https://search. ebscohost.com/login.aspx?direct=

true&AuthType=ip,shib&db=edsair&AN =edsair. doi..........e01c3e2cbbc568d5c9ab5c45 81ac604b&authtype=shib&lang=cs&site=eds-live&scope=site&authtype=shib& custid=s7108593

Peris, M., de la Barrera, U., Montoya-castilla, I., & Schoeps, K. (2020). Psychological risk factors that predict social networking and internet addiction in adolescents. *International Journal of Environmental Research and Public Health*, *17*(12), 1 - 23. https://doi.org/10.3390/ijerph17124598

Průcha, J., & Míka, J. (2000). *Distance learning in questions (guide for students and those interested in studying)*. CSVŠ - National Center for Distance Education.

Riesmeyer, C., Naab, T., Camerini, A., Festl, R., & Dallmann, C. (2019). Zwischen Selbstoffenbarung und elterlicher Social-Media-Treuhänderschaft: Wie Eltern mit den digitalen Identitäten ihrer Kinder umgehen. *MedienPädagogik: Zeitschrift für Theorie und Praxis der Medienbildung*, (35), 97-115. https://search.ebscohost.com/login.aspx?direct=true&AuthType=ip,shib&db=edsoai&AN=edsoai.on1135342921&lang=cs&site=eds3live&scope=site&authtype=shib&custid=s7108593

Všetulová, M., Nocar, D., Urbášková, L., Dvořáková, M. (2007). *Tutor's Guide. Olomouc: Academy of Distance Education.*

Zlámalová, H. (2007). Distance education - yesterday, today and tomorrow. *E-Pedagogium*, *7*(3), 29-44. https://e-pedagogium.upol.cz/pdfs/ epd/2007/03/04.pdf

Zhu, C., Huang, S., Evans, R., & Zhang, W. (2021). Cyberbullying among adolescents and children: A comprehensive review of the global situation, risk factors, and preventive measures. Frontiers in public health, 9, 634909.