Studia Prawnicze. Rozprawy i Materiały 2021, nr 1 (28) • Studies in Law: Research Papers 2021, No. 1 (28)
ISSN 1689-8052 • e-ISSN 2451-0807

DOI: 10.34697/2451-0807-sp-2021-1-009

Artur Kapera
Private Academic High School no. 8 in Kraków
ORCID: 0000-0002-5090-9197
kaperaa@protonmail.com

Jacek Kapera
Mszana Dolna Engineering and Information Technology School Complex, Poland
ORCID: 0000-0003-2044-9158
kaperaa@protonmail.com

Internet-related risks from the perspective of Polish adolescents with a focus on hate speech

Introduction

With the growing importance of the Internet, threats are emerging and their magnitude on the web increases. Young people are particularly vulnerable. It is therefore necessary to monitor and attempt to prevent these problems. The analysis of available literature shows that the majority of papers in the field are reports and that there are still few up-to-date scientific studies on individual risks analysed on a case-by-case basis. In addition, in-depth studies on young people's online activities have a relatively short history.[1] Meanwhile, the look presented in the article may contribute to a deeper understanding of the nature of these problems. Taking into account the above considerations, the main risks associated with the use of the Internet by the Polish youth were presented, and then the issue of hate speech was analysed. In the research procedure, in the first year, a review of source materials was carried out, and then a questionnaire was prepared for young people attending upper secondary schools. The authors'

[1] K. Abramczuk, J. Pyżalski, A. Zdrodowska, Ł. Tomczyk, *Polskie badanie EU Kids Online 2018. Najważniejsze wyniki i wnioski*, WN UAM, Poznań 2018, p. 7, https://fundacja.orange.pl/files/user_files/EU_Kids_Online_2019_v2.pdf [accessed: 10.05.2019].

own observations were also helpful, as well as the authors' experience related to the administration of computer networks and work with teenagers.

The aim of the study was to present the main threats related to the use of the Internet by the Polish youth and to analyse it with a special emphasis on issues related to hate speech.

Risks on the Internet

The usefulness of the Internet is currently undisputed. In Poland, in 2018, according to CSO data, 77.5% of the Polish population uses the Internet, 74.8% of people use it at least once a week.[2] In the same year, 82.7% of households had at least one computer at home.[3] According to the Central Statistical Office, households with children have access to the Internet more often than households with no children.[4]

The Internet, being in fact a network of interconnected computers, carries with it the possibility of the emergence of many threats, which can be dangerous for both the users and the computer equipment. A number of different classifications based on specific criteria are present in this field's literature. One example is the typology proposed by Wójcik[5] developed on the basis of Livingstone, Haddon, Görzig and Olafsson[6].

This article describes the following issues, with particular emphasis on hate speech:

- malware (including spyware, ransomware, crypto-miners and adware);
- phishing;
- targeted hacker attacks;
- spam;
- violation of user privacy (by corporations and governmental organizations);
- paedophilia and paedophilic content;

---

2 Główny Urząd Statystyczny, *Społeczeństwo informacyjne w Polsce w 2018 r.*, 22.10.2018, https://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/5497/2/8/1/spoleczenstwo_informacyjne_w_polsce_w_2018_roku.pdf [accessed: 10.05.2019].

3 *Ibidem*.

4 *Ibidem*.

5 S. Wójcik, *Zagrożenia dzieci i młodzieży w internecie*, „Dziecko Krzywdzone. Teoria. Badania. Praktyka" 2017, nr 16 (1), https://bazhum.muzhp.pl/media/files/Dziecko_Krzywdzone_teoria_badania_praktyka/Dziecko_Krzywdzone_teoria_badania_praktyka-r2017-t16-n1/Dziecko_Krzywdzone_teoria_badania_praktyka-r2017-t16-n1-s270-287/Dziecko_Krzywdzone_teoria_badania_praktyka-r2017-t16-n1-s270-287.pdf [accessed: 8.05.2021].

6 A. Görzig, L. Haddon, S. Livingstone, K. Olafsson, *EU kids online: final report*, London School of Economics & Political Science, London 2011, http://eprints.lse.ac.uk/39351/1/EU_kids_online_final_report_%5BLSERO%5D.pdf [accessed: 8.05.2021].

- human sex trafficking;
- hate speech ("hejt");
- cyber-bullying in general (elements not included in other categories such as hate speech).

Table 1: Typology of threats to children online

	Sex	**Aggression**	**Other threats**	**Commerce**
Content – the child as a recipient	Pornography	Depictions of violence	Other harmful content	Fraudulent marketing, spam
Contact – the child as a participant	Grooming	Electronic aggression	Ideological and anti-health persuasion	Identity theft
Conduct – the child as a perpetrator	Sexting	Perpetration of electronic aggression	Production of harmful content	Hacking, piracy

Source: adapted and translated from: S. Wójcik, *Zagrożenia dzieci i młodzieży w internecie*, "Dziecko Krzywdzone. Teoria. Badania. Praktyka" 2017, nr 16 (1), https://bazhum.muzhp.pl/media/files/Dziecko_Krzywdzone_teoria_badania_praktyka/Dziecko_Krzywdzone_teoria_badania_praktyka-r2017-t16-n1/Dziecko_Krzywdzone_teoria_badania_praktyka-r2017-t16-n1-s270-287/Dziecko_Krzywdzone_teoria_badania_praktyka-r2017-t16-n1-s270-287.pdf [accessed: 8.05.2021].

The following is a description of each of the risks listed, with particular attention paid to the hate speech.

Malware is a combination of the words "malicious" and "software", which are programs and scripts designed for purposes harmful to the victim, such as stealing personal data – spyware, forcing payment for previously encrypted documents – ransomware, using computer resources to mine cryptocurrencies – crypto-miners and displaying advertisements throughout the operating system – adware[7].

Phishing is a name used to describe the impersonation of known companies or private entities in order to obtain information from the user. Email is a common medium for phishing, as it is not difficult to change the sender's address to the address of a large company[8].

A targeted hacking attack can be defined as "An assault on system security that derives from an intelligent threat, i.e., an intelligent act that is a deliberate attempt (especially in the sense of a method or technique) to evade security ser-

[7] INTELi SERWIS, *Co to jest szkodliwe oprogramowanie*, 13.08.2013, http://inteliserwis.szczecin.pl/co-to-jest-szkodliwe-oprogramowanie [accessed: 10.05.2019].

[8] A. Ścibor, *Czym jest phishing?*, AVLab Cybersecurity Foundation, https://avlab.pl/czym-jest-phishing [accessed: 10.05.2019].

vices and violate the security policy of a system. [...] On the Internet, potential outside attackers range from amateur pranksters to organized criminals, international terrorists, and hostile governments".[9]

According to the Merriam-Webster dictionary, spam can be defined as "unsolicited usually commercial messages (such as e-mails, text messages, or Internet postings) sent to a large number of recipients or posted in a large number of places".[10] According to SpamCop's statistics, 82 648 926 spam messages have been reported during the last year alone, with the highest values set at 4.7 reports per second.[11]

The right to privacy is a fundamental human right and should be respected. Despite that, as Rezgui. Bouguettaya and Eltoweissy say, "the ease of information access, coupled with the ready availability of personal data, also made it easier and more tempting for interested parties (individuals, businesses, and governments) to intrude on people's privacy."[12] Privacy intrusion by businesses is often performed in order for them to be able to provide customized services and products. It is worth noting that customers often do not know explicitly authorize such data collection practices. Governmental organizations also collect a large amount of data about a given country's citizens.[13]

Paedophilia on the Internet can manifest itself in many forms, mostly either through distribution of child pornography or "online predators" — people who use the Internet to coerce children into meeting with them and then assault their victims[14].

Human sex trafficking is defined as "[...] a form of modern slavery. Criminals of sex trafficking such as pimps, johns, and madams use violence, threats, lies, money, drugs, and other forms of coercion to compel or force children and adults to engage in unwanted sexual acts against their will."[15]

---

9 R. Shirey, *Internet Security Glossary*, Internet Society 2000, p. 13.

10 Merriam Webster, *Spam* [headword], https://www.merriam-webster.com/dictionary/spam [accessed: 10.05.2019].

11 *SpamCop statistics*, spamcop.net, https://www.spamcop.net/spamgraph.shtml?spamyear [accessed: 10.05.2019].

12 A. Bouguettaya, M. Eltoweissy, A. Rezgui, *Privacy on the Web: Facts, Challenges, and Solutions*, "IEEE Security & Privacy Magazine" 2003, vol. 1 (6), pp. 40–41.

13 *Ibidem*.

14 P. Corriveau, Ch. Greco, *Online Pedophilia and Cyberspace*, Institut national de sante publique Quebec, https://www.inspq.qc.ca/en/sexual-assault/fact-sheets/online-pedophilia-and-cyberspace [accessed: 10.05.2019].

15 E. Sznitka, *Human Trafficking and the Internet*, The Child Advocacy Center of Lapeer County, https://www.caclapeer.org/lapeercacblog/human-trafficking-the-internet [accessed: 10.05.2019].

Hate speech and cyber-bullying

The term "hate speech" has been increasingly often used on the Internet and in other media over recent years. This is related to the increase of the phenomenon on the Internet. In this context, there are attempts to study it and find ways to counteract such behaviours, demonstrated both by various organizations and by scientists themselves. In Poland, the issue was the subject of reflections conducted e.g. by Włodarczyk as part of the project "Internet without hate"[16] , in which, however, as the author notes, the universality of this issue "may reduce young people's sensitivity to the problem".[17] The topic was also addressed in other analyses, including the Minority Report ("Raport mniejszości"), which addressed the monitoring of content by Internet users, covering the identification of content aggressive towards ethnic, sexual, religious and other minorities[18], and the report "Internet culture of offence", in which it is emphasized that although the Internet has the most unfavourable image among other media in the analysed context, nonetheless still "crossing cultural boundaries online remains a marginal phenomenon".[19] An attempt to explore the behaviour of young people on the Internet is made within the framework of the EU Kids Online study, in which Poland also participates. The document takes into account chosen issues at a specific level of detail. Meanwhile, this study highlights the issues of hate speech. The analysis of available sources allows one to see that the subject matter of the discussed issue concerns mainly: attempts to define the issue, its characteristics and the scale of the problem and proposing solutions. As far as the definition of hate speech in this paper is concerned, it is assumed that hate speech is "any form of expression that spreads, promotes or justifies racial hatred, xenophobia, anti-Semitism and other forms of hatred based on intolerance, including, but not limited to intolerance expressed in aggressive nationalism and ethnocentrism, discrimination and hostility towards minorities as well as immigrants and people of immigrant origin."[20] The phenomenon

---

16 J. Włodarczyk, *Mowa nienawiści w internecie w doświadczeniu polskiej młodzieży*, „Dziecko Krzywdzone. Teoria. Badania. Praktyka" 2014, nr 13 (2).

17 *Ibidem*.

18 Fundacja Wiedza Lokalna, https://prepedia.fandom.com/wiki/Fundacja_Wiedza_Lokalna [accessed: 10.05.2019].

19 *Internetowa kultura obrażania*, 2016/2017, IAB Polska, p. 3, https://iab.org.pl/wp-content/uploads/2017/05/InternetowaKulturaObrazania_2016_2017_raport_20170511.pdf [accessed: 10.05.2019].

20 *Recommendation No. R (97) 20 of the Committee of Ministers to Member States on "hate speech"*, Council of Europe, adopted on 30 October 1997, p. 107; *Recommendation N°6: Combating the dissemination of racist, xenophobic and antisemitic material via the internet*, *Additional Protocol to the Cybercrime Convention,* Council of Europe, adopted on 15 December 2000.

is associated with the notions of "hating, often understood in a broader sense than hate speech itself,[21] which stands for offensive online content, usually affecting specific people.[22] In the subject's literature, both terms are understood in different ways and are generally treated interchangeably by the average young Internet user. On this basis, they have been treated collectively in the research. The issue of cyber-bullying is also related to the discussed subject matter. It is defined as "violence using information and communication technologies".[23] In the context of the subject matter discussed, it is also difficult not to describe the concept of so-called trolls, whose activities include publishing aggressive content and negative comments. Hate speech is visible on, among other things, websites, blogs and Internet forums, e-mail or social media, as well as in the case of comments appearing under articles on the Internet, film, music or games.

Internet users can and should respond to hate speech online. First of all, they can be reported to service administrators. In turn, taking into account the legal issues in the Polish legislation on the prohibition of activities that allow racial and national hatred is referred to in the Constitution of the Republic of Poland.[24] The fact that hate speech is punishable derives from the Criminal Code.

Article 256

§ Whoever publicly promotes a fascist or other totalitarian state system or incites hatred on the grounds of nationality, ethnicity, race, religion or because of non-confessionality, shall be subject to a fine, the penalty of restriction of liberty or the penalty of imprisonment for up to 2 years.

§ Whoever produces, preserves or imports, acquires, stores, possesses, presents, transports or sends a print, recording or other object containing the content specified in § 1 or being a carrier of fascist, communist or other totalitarian symbolism for the purpose of distribution shall be subject to the same penalty.[25]

---

[21] *Bezpieczeństwo dzieci online. Kompendium dla rodziców i profesjonalistów*, Polskie Centrum Programu Safer Internet, Warszawa 2018, p. 43, https://www.edukacja.fdds.pl/dd5bcf09-cf2d-4340-9eb3-2c437ef66245/Extras/ksiazka-Bezpieczenstwo_dzieci_online_Kompendium_dla_rodzicow_i_profesjonalistow-FDDS-12042017.pdf [accessed: 10.05.2019].

[22] *Internetowa kultura obrażania...*, *op. cit*., p. 3.

[23] Ł. Wojtasik, *Cyberprzemoc – charakterystyka zjawiska, skala problemu, działania profilaktyczne*, kampania „Dziecko w Sieci", https://www.sp118.pl/userdata/projekty/internet/cyberprzemoc.pdf [accessed: 10.05.2019].

[24] Konstytucja Rzeczypospolitej Polskiej, Art. 32, Dz. U. 1997, Nr 78, poz. 483 z późn. zm.

[25] Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz. U. 1997, Nr 88 ,poz. 553 z późn. zm., p. 29.

Article 257

Whoever publicly insults a group of people or a particular person because of their national, ethnic, racial, or religious affiliation, or because of their lack of religious beliefs, or for such reasons violates the physical inviolability of another person, shall be subject to the penalty of imprisonment for up to 3 years.[26]

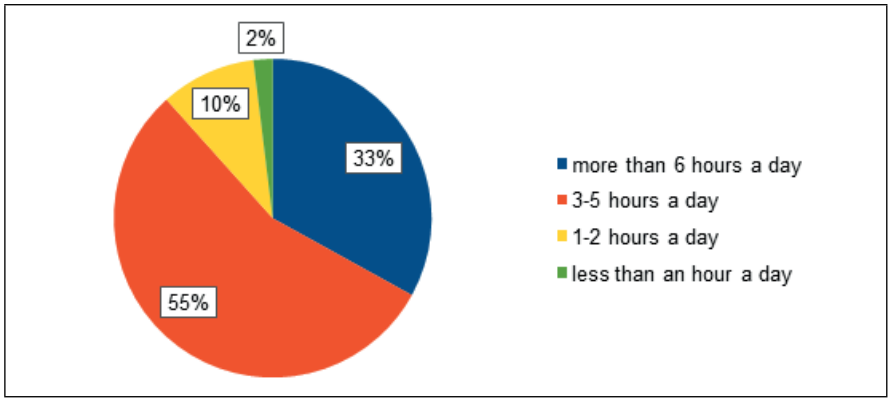
Scientific approach and research sample

A diagnostic survey based on a questionnaire consisting of 26 questions was used in the research procedure. Pilot studies were conducted in the period from February to April 2019 in three units in the Małopolskie Voivodeship. These were schools: VIII Private Academic High School in Cracow, Józef Marek High School Complex in Mszana Dolna and Technical and Information Technology School Complex in Mszana Dolna. Such a selection of schools allowed for differentiation resulting from the private and public character of schools, and was also related to the educational profile of the units in question. The survey involved 48 women and 54 men that lived in the Małopolskie Voivodeship.

Study results

All respondents admitted that they use the Internet every day. Most of them use the Internet for 3–5 hours every day (Figure 1).

Figure 1: Frequency of Internet use by respondents

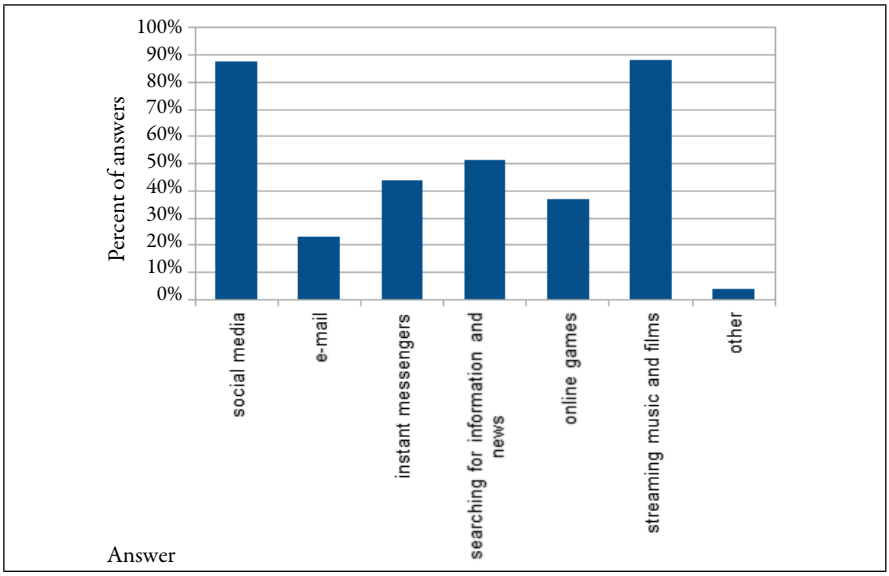


Source: Own analysis based on surveys.

[26] *Ibidem*.

For the most part, young people use the Internet at home. They mainly use the following Internet tools: social media and websites to watch films and listen to music (Figure 2).

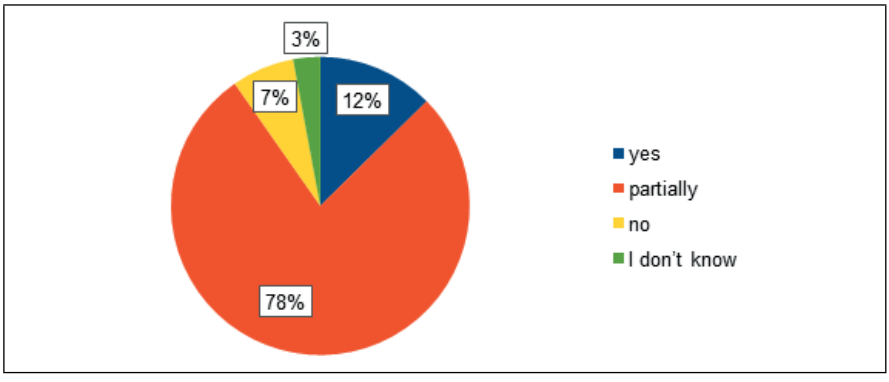
Figure 2: Internet services used by respondents



Source: Own analysis based on surveys.

The majority of respondents considered the use of the Internet to be only partially safe (Figure 3).

Figure 3: Summary of responses to the question whether the respondents considered using the Internet to be safe

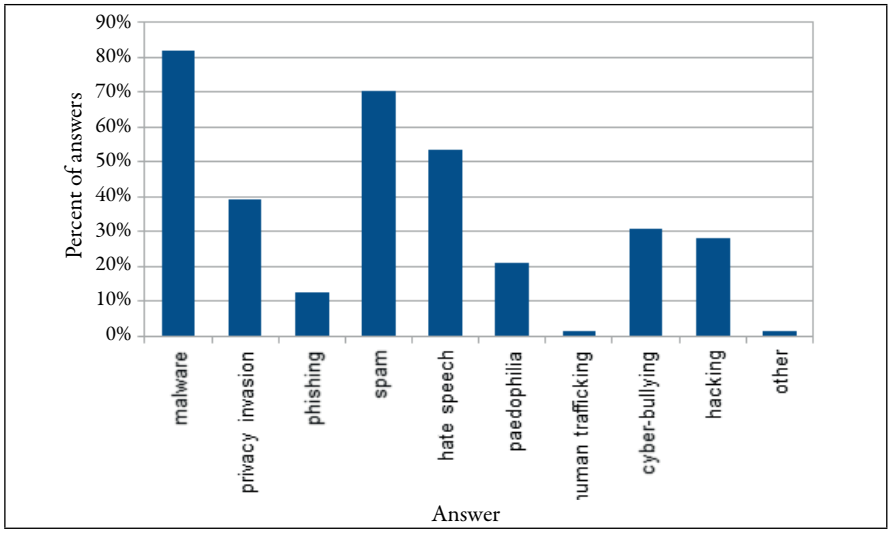


Source: Own analysis based on surveys.

Respondents identified viruses (malware), theft/leakage of personal data, hackers, fraud, "people" / "human stupidity" and paedophilia as the biggest threats on the Internet.

69% of the respondents, who surfed the web, encountered threats. These were mainly malware and spam (Figure 4).

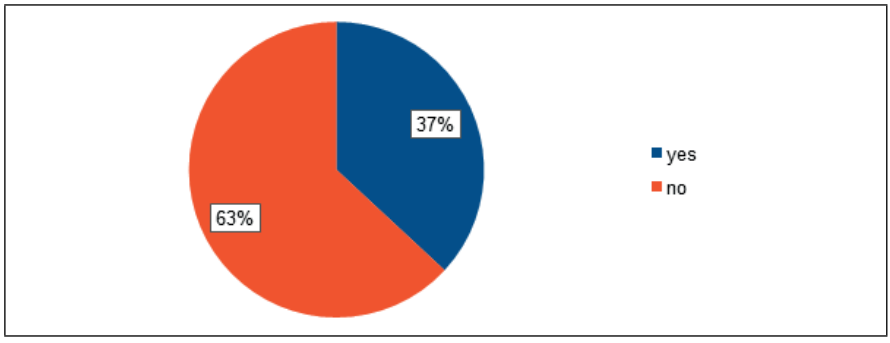
Figure 4: Threats encountered by respondents when using the Internet



Source: Own analysis based on surveys.

Respondents were also asked if they had ever been subjected to hate speech. 37% of respondents said they were a victim (Figure 5).

Figure 5: Summary of responses to the question concerning the use of hate speech towards the respondents



Source: Own analysis based on surveys.

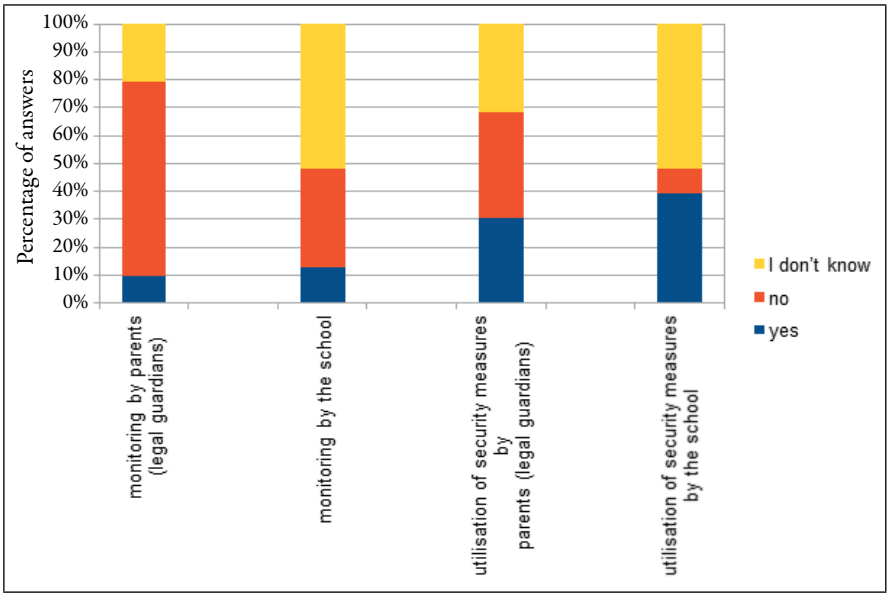
Hate speech encounters most often occurred during the usage of social media and online games. At the same time, nearly 18% of young people admitted that they themselves used hate speech on the Internet, as their motive mentioning mainly nervousness, anger and sudden emotions.

Respondents propose ways to fight against hate speech, including for example: limiting access to the Internet, self-control and restraint, as well as reporting or ignoring people using hate speech and letting site moderators warn or block them.

Further questions in the questionnaire were specifically targeted at cyber-security issues. Young people were asked if they used tools to protect themselves against threats. Most of them said they did. Among the most frequently used ones are: antiviruses, strong passwords, programs and plug-ins used to block advertisements, programs creating VPNs (virtual private networks) and common sense.

Subsequent questions concerned the existence of monitoring and protection against risks on the Internet in schools and at home. In the first case, young people say that their online activity is not monitored by parents (legal guardians), and in the case of schools they do not have such knowledge. As far as security measures are concerned, as before, in the case of schools they do not know about such security measures, and in the case of parents the responses were distributed evenly (Figure 6).

Figure 6: Monitoring of activity and application of security measures against threats on the Internet



Source: Own analysis based on surveys.

Discussion and conclusion

Young people identified viruses (malware), theft/leakage of personal data, hackers, fraud, "people" / "human stupidity" and paedophilia as the biggest threats on the Internet. More than a third of them are people who have been subjected to hate speech on the web. At the same time, close to – indicated that they were engaged in such activity. According to the EU Kids Online survey, almost half of young people use the Internet for up to two hours on weekdays and up to three hours at weekends, with the most frequent use being for entertainment.[27] The authors of the report also point out that one in three teenagers encountered hate or humiliation, or comments directed against specific people or groups of people, in the last year, and nearly 6% of them declared sending at least one such message directed against other people, indicating religion, physical appearance and religion as the main reason.[28] The frequency of encountering hate speech content on the Internet is also confirmed by the research conducted by the Stefan Batory Foundation, which shows that 70% of young people encountered racist statements.[29]

The research conducted by the Nobody's Children Foundation (Fundacja Dzieci Niczyje) shows that the phenomenon of hate speech affects 40% of young people aged 14–17 (such a percentage of people encountered manifestations of hate speech), including 45% of people in the group of 16-17 years of age.

Other analyses indicate that 0.5–0.9% of posts on the Internet cross cultural borders, and Internet users themselves admit only a few percent cross cultural borders by using vulgar language or insulting other people, although the image of the Internet itself seems to contradict these observations[30]. Nevertheless, the respondents suggested ways to fight against hate speech, for example: restricting access to the Internet, self-control and composure, as well as reporting or ignoring persons using hate speech and letting site moderators warn or block them. Respondents generally feel only partially safe surfing the web. The above observations are largely confirmed by other authors.

According to the EU Kids Online report, 65% of young people feel often or always safe online.[31] However, it is difficult to determine to what extent the

---

27 K. Abramczuk J. Pyżalski, A. Zdrodowska, Ł. Tomczyk, *op. cit.*, p. 22, 33.

28 *Ibidem*.

29 M. Bilewicz, M. Marchlewska, W. Soral, M. Winiewski, *Mowa nienawiści. Raport z badań sondażowych*, Fundacja im. Stefana Batorego, Warszawa 2014, p. 4, http://www.ngofund.org.pl/wp-content/uploads/2014/06/raport-na-formacie-B5_19.11.14.pdf [accessed: 10.05.2019].

30 *Internetowa kultura obrażania...*, *op. cit*., p. 3.

31 K. Abramczuk, J. Pyżalski, A. Zdrodowska, Ł. Tomczyk, *op. cit*., p. 89.

declared sense of security results from ignorance of the scale of threats accompanying network users, and to what extent it is connected with a certain acceptance of the phenomena occurring on the Web.

Parents, school and educational institutions, as well as government agencies, social organizations and public services have a huge role to play in the issue of safety of children and young people on the Internet. In this respect, parents should first of all talk to their children and inform them about the risks. In addition, they can also take other actions – block access to harmful content, restrict access to specific programs or devices, and monitor the child's activity on the Internet.[32] As the report referred to above has shown, the most frequently used methods include providing advice on Internet safety.[33] However, 55.6% of young people surveyed admit that their parents are not interested in how they use the Internet.[34] Another issue is the safety of young people online during school hours. Previous analyses have shown that almost one in three older students, once a week or more often, look for information on the school website or on the school's e-learning platform.[35] In this context, the ability to ensure online security is a challenge for any modern school. Meanwhile, almost 60% of pupils say that the teacher has not talked to them about what they are doing online.[36] Therefore, it is important to train teachers. In the discussed context, both the regulations contained in the educational law and internal regulations, characteristic for a given unit, as well as curricula, educational and preventive programmes are also important. Apart from legal aspects, the best way to deal with threats on the Internet, including hate speech, still seems to be the education of Internet users. However, in order for education to be effective, further research is needed, also in other age groups and on a wider territorial scale.

Bibliography

Abramczuk K., Pyżalski J., Tomczyk Ł., Zdrodowska A., *Polskie badanie EU Kids Online 2018. Najważniejsze wyniki i wnioski*, WN UAM, Poznań 2018, https://fundacja.orange.pl/files/user_files/EU_Kids_Online_2019_v2.pdf [accessed: 10.05.2019].

Bilewicz M., Marchlewska M., Soral W., Winiewski M., *Mowa nienawiści. Raport z badań sondażowych*, Fundacja im. Stefana Batorego, Warszawa 2014, http://www.ngofund.org.pl/wp-content/uploads/2014/06/raport-na-formacie-B5_19.11.14.pdf [accessed: 10.05.2019].

[32] *Bezpieczeństwo dzieci online...*, *op. cit.*, p. 43.

[33] K. Abramczuk, J. Pyżalski, A. Zdrodowska, Ł. Tomczyk, *op. cit*., p. 56.

[34] *Nastolatki wobec Internetu*, Wyższa Szkoła Nauk Społecznych Pedagogium – Rzecznik Praw Dziecka, Warszawa 2014, https://akademia.nask.pl/badania/raport_z_badan_nastolatki_wobec_internetu.pdf [accessed: 10.05.2019].

[35] K. Abramczuk, J. Pyżalski, A. Zdrodowska, Ł. Tomczyk, *op. cit*., p. 47.

[36] *Ibidem*, p. 49.

Bezpieczeństwo dzieci online. Kompendium dla rodziców i profesjonalistów, Polskie Centrum Programu Safer Internet, Warszawa 2018, https://www.edukacja.fdds.pl/dd5bcf09-cf2d-4340-9eb3-2c437ef66245/Extras/ksiazka-Bezpieczenstwo_dzieci_online_Kompendium_dla_rodzicow_i_profesjonalistow-FDDS-12042017.pdf [accessed: 10.05.2019].

Bouguettaya A., Eltoweissy M., Rezgui A., *Privacy on the Web: Facts, Challenges, and Solutions*, "IEEE Security & Privacy Magazine" 2003, vol. 1 (6).

Corriveau P., Greco Ch., *Online Pedophilia and Cyberspace*, Institut national de sante publique Quebec, https://www.inspq.qc.ca/en/sexual-assault/fact-sheets/online-pedophilia-and-cyberspace [accessed: 10.05.2019].

Główny Urząd Statystyczny, *Społeczeństwo informacyjne w Polsce w 2018 r.*, 22.10.2018, https://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/5497/2/8/1/spoleczenstwo_informacyjne_w_polsce_w_2018_roku.pdf [accessed: 10.05.2019].

Görzig A., Haddon L., Livingstone S., Olafsson K., *EU kids online: final report*, London School of Economics & Political Science, London 2011, http://eprints.lse.ac.uk/39351/1/EU_kids_online_final_report_%5BLSERO%5D.pdf [accessed: 8.05.2021].

Internetowa kultura obrażania, 2016/2017, IAB Polska, https://iab.org.pl/wp-content/uploads/2017/05/InternetowaKulturaObrazania_2016_2017_raport_20170511.pdf [accessed: 10.05.2019].

Konstytucja Rzeczypospolitej Polskiej, Art. 32, Dz. U. 1997, Nr 78, poz. 483 z późn. zm.

Merriam Webster, *Spam* [headword], https://www.merriam-webster.com/dictionary/spam [accessed: 10.05.2019].

Nastolatki wobec Internetu, Wyższa Szkoła Nauk Społecznych Pedagogium – Rzecznik Praw Dziecka, Warszawa 2014, https://akademia.nask.pl/badania/raport_z_badan_nastolatki_wobec_internetu.pdf [accessed: 10.05.2019].

Recommendation No. R (97) 20 of the Committee of Ministers to Member States on "hate speech", Council of Europe, adopted on 30 October 1997.

Recommendation N°6: Combating the dissemination of racist, xenophobic and antisemitic material *via* the internet, Additional Protocol to the Cybercrime Convention, Council of Europe, adopted on 15 December 2000.

Shirey R., *Internet Security Glossary*, Internet Society 2000, https://www.rfc-editor.org/rfc/pdfrfc/rfc2828.txt.pdf [accessed: 10.05.2019].

Spamcop statistics, spamcop.net, https://www.spamcop.net/spamgraph.shtml?spamyear [accessed: 10.05.2019].

Sznitka E., *Human Trafficking and the Internet*, The Child Advocacy Center of Lapeer County, https://www.caclapeer.org/lapeercacblog/human-trafficking-the-internet [accessed: 10.05.2019].

Ścibor A., *Czym jest phishing?*, AVLab Cybersecurity Foundation, https://avlab.pl/czym-jest-phishing [accessed: 10.05.2019].

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz. U. 1997, Nr 88, poz. 553 z późn. zm.

Włodarczyk, J. *Mowa nienawiści w internecie w doświadczeniu polskiej młodzieży*, „Dziecko Krzywdzone. Teoria. Badania. Praktyka" 2014, nr 13(2).

Wojtasik Ł., *Cyberprzemoc – charakterystyka zjawiska, skala problemu, działania profilaktyczne*, kampania „Dziecko w Sieci", https://www.sp118.pl/userdata/projekty/internet/cyberprzemoc.pdf [accessed: 8.05.2021].

Wójcik S., *Zagrożenia dzieci i młodzieży w internecie*, „Dziecko Krzywdzone. Teoria. Badania. Praktyka" 2017, nr 16 (1), https://bazhum.muzhp.pl/media/files/Dziecko_Krzywdzone_teoria_badania_praktyka/Dziecko_Krzywdzone_teoria_badania_praktyka-r2017-t16-n1/Dziecko_Krzywdzone_teoria_badania_praktyka-r2017-t16-n1-s270-287/Dziecko_Krzywdzone_teoria_badania_praktyka-r2017-t16-n1-s270-287.pdf [accessed: 8.05.2021].

Fundacja Wiedza Lokalna, https://prepedia.fandom.com/wiki/Fundacja_Wiedza_Lokalna [accessed: 10.05.2019].

Abstract

Internet-related risks from the perspective of Polish adolescents with a focus on hate speech

The aim of the study was to present the main threats related to the use of the Internet by the Polish youth and to analyse them with particular emphasis on issues related to hate speech. Using the Internet, apart from its undoubted usability, brings with it a number of threats, among which are: malware (including spyware, ransomware, "crypto-miners" and adware), invasion of privacy (both by private individuals (stalking) and advertising companies), phishing, spam, hate speech, paedophilia, human trafficking, cyber-bullying, and, less frequently, targeted attacks. According to the survey, nearly 70% of the respondents encountered threats on the Internet. The phenomenon of hate speech affects 37% of respondents who fell victim to it and 18% who practised hate speech.

Key words: Internet, security, hate speech, privacy