Contemporary Educational Technology, 2025, **17**(1), ep546
ISSN: 1309-517X (Online)

OPEN ACCESS

Research Article

Online attacks on teachers versus strategies to address cyberbullying and cyberaggression in the school ecosystem

Łukasz Tomczyk [1*]
0000-0002-5652-1433

[1] Jagiellonian University, Cracow, POLAND
[*] Corresponding author: lukasz.tomczyk@uj.edu.pl

Citation: Tomczyk, Ł. (2025). Online attacks on teachers versus strategies to address cyberbullying and cyberaggression in the school ecosystem. *Contemporary Educational Technology, 17*(1), ep546. https://doi.org/10.30935/cedtech/15663

ARTICLE INFO

Received: 23 Jun 2024
Accepted: 6 Nov 2024

ABSTRACT

The aim of the article is to present ways of resolving the situations related to cyberbullying and cyberaggression that occur in Polish schools. The research fills a gap (taboo subject) in the means of solving crisis situations related to attacks on teachers that occur online. The qualitative research (online interviews) conducted in Poland at the end of 2023 and the beginning of 2024 involved teachers who had been attacked by students and/or parents because of their profession. On the basis of the analysis and categorization (in the grounded theory stream), nine strategies were identified: educational and preventive actions targeted at students; working with the student's family; removal of harmful content from the Internet; independent action by teachers; notifying the police; involvement of judicial authorities; individual consequences for the student; a combination of these different forms; and no response to the cyber-attack. The research was carried out as part of the digitally safer teacher project and is characterized by a praxeological dimension related to the special attention paid to the protection of teachers in cyberspace.

Keywords: attacks, cyberbullying, cyberaggression, teachers as victims, students, parents, school

INTRODUCTION

Research and action on the reduction of risk behavior in the new media space has now become one of the core components of the rapidly-developing media pedagogy (Mihailidis et al., 2021; Tomczyk, 2023). The irreversible digitization of everyday life brings many benefits, improves communication processes, and speeds up private and professional tasks, but can also create problematic situations (Pfaffinger et al., 2020). Among such situations, many risk behaviors mediated by digital media have emerged, such as problematic use of the Internet, vulnerability to manipulation and false information, and being exposed to online attacks in the form of cyber-aggression or cyber-bullying (Bjelajac et al., 2022; Romero Rodrigo et al., 2021). Among the e-risks, there is a group of risks that can be minimized through the possession and development of the appropriate competences and knowledge. There is also a set of e-risks that, regardless of digital and media competence, are difficult to anticipate and are also characterized by their highly destructive impact. This second group of problematic phenomena can include attacks mediated by new media that are conducted intentionally and involve negative emotional and image consequences or, in extreme cases, result in legal liability (Bostancı Bozbayındır, 2019; Marín-López & Zych, 2024).

Young people are particularly vulnerable to cyberbullying and cyberaggression (Mascia et al., 2021; Saladino et al., 2020). The phenomenon is well understood in terms of its magnitude and the mechanisms that accompany peer harassment through information and communication technologies (ICTs) (Jaskulska et al., 2022). For more than two decades, this topic has been explored to great depths by educators and media psychologists who, based on scientific evidence, propose a number of preventive solutions that pre-empt the phenomena of online bullying or address the problem when it occurs (Pyżalski et al., 2022). However, despite the rich literature on the subject, there is an empirical gap related to delineating an up-to-date typology of

strategies for solving this type of problematic situation among in-service teachers. It should be emphasized that while the phenomena of the Internet-mediated attacks by parents and students are encountered by only a few to several percent (Kopecký & Szotkowski, 2017), the literature so far does not discuss how to address this type of problematic situation in educational institutions from the perspective of the educator as victim. The emphasis on prevention and the approaches to solving this type of problematic situation is on young people (Sanders, 2022) and does not sufficiently include teaching staff (Rajbhandari & Rana, 2022; Zăvoianu & Sun, 2022). In view of the above, this article fills a gap in the research of the whole-school ecosystem in the context of cyberbullying and cyberaggression, while also providing a voice in the discussion on digital safety for teachers.

OVERVIEW OF STUDIES

Research on cyberbullying and cyberaggression is currently characterized by a lack of validity regarding the scale of the different forms of attack that targets teachers (Tomczyk et al., 2024a). Diagnoses are not carried out in a way that makes it possible to show the change in the dynamics of the phenomenon, or to show its scale by continent, country, or region. However, based on historical data, it is known that one in five teachers in the Czech Republic experienced an online attack in 2016 (Kopecký & Szotkowski, 2017). In contrast, a study carried out in Finland found that 30% of research and teaching staff from higher education institutions had been victims of online harassment within a six-month period. Those active in social and traditional media, as well as those in senior positions, were more likely to be the target of a variety of attacks (Oksanen et al., 2021). In general, when analyzing the results of research on cyberbullying and cyberaggression–defined in this manuscript as online attacks–one should be aware that the available research reports do not allow conclusions to be drawn regarding the current scale and mechanisms of the phenomenon. The fact that it is a taboo subject does not facilitate the realization of such diagnoses either.

Online attacks targeting teachers can take a variety of forms: the spreading of false information in online spaces, direct attack using online tools, recording teachers without their consent, online blackmail, creating and spreading memes with different levels of harmfulness, photoshopping (including with sexual content), covert cyberbullying (occurring on newsgroups inaccessible to the teacher), destructive actions within e-learning, creating fake teacher profiles, and using digital tools to attack offline spaces, along with other possible forms of attack (Tomczyk et al., 2024a). A study by researchers in Nepal expands this palette of attacks targeting teachers to include trivially belittling the teacher's knowledge and professional competence on social media, sending unethical requests from parents and students, sending requests of a sexual nature, sending 'cheeky' (outside social norms) comments and messages, sabotaging content shared by teachers, and trolling and manipulating content shared by teachers in online spaces (Rajbhandari & Rana, 2022). Different types of attack require different forms of response to a diverse range of behaviors aimed at creating negative emotions and damaging the image of the teacher. Each of the aforementioned forms of attack also gives rise to different legal implications (Pennell et al., 2021; Thompson, 2021) and require teachers and school leaders to possess interdisciplinary knowledge and digital competences (Fredrick et al., 2023; Macaulay et al., 2018).

Teachers' digital competences provide a starting point for anticipating cyber-attacks (Torres-Hernández & Gallego-Arrufat, 2022), as well as enabling them to minimize the negative consequences of attacks they may face due to their profession. Technical skills are intertwined in the case of self-protection in cyberspace (Šimandl & Vaníček, 2017) with knowledge of the mechanisms of cyberbullying and cyberaggression, as well as legal knowledge (Arifin, 2020; Schimmel & Militello, 2007). In particular, the last of these protective factors is useful in the situation of a direct attack through ICTs, in which a teacher's good name is compromised, or a school employee feels that the threat created online may translate into a risk against their safety in the offline space (Bo & Onwubuya, 2022). These two areas related to digital and media literacy and legal knowledge are a starting point in the analysis of teacher safety in an increasingly digitalized school. Nevertheless, it is important to be aware that the two areas are not sufficient to cover the whole range of activities and actors that support teachers in a crisis situation or provide a basis for e-threat prevention (Tomczyk, 2024).

From the residual findings, an interesting picture emerges of the ways in which teachers who have experienced online attacks cope. Among such solutions they mention: discussing the situation with immediate family members, taking advice from other teachers, attempting to find the inner strength to

resolve the situation themselves, attempting to contact the student behind the problem and situating it in the wider context, developing knowledge and skills 'in stock' to feel safe, limiting contact with students in online spaces, in extreme cases changing their place of work, introducing clear regulations at the school, and the threat of punishment for the student (Rajbhandari & Rana, 2022). The solutions proposed are suggestions that point to both addressing such problems using one's own resources and those inherent in the professional and personal environment. However, given the complexity of the factors behind online attacks, such as moral disengagement, low awareness of online risks, and a generally negative school climate (Sorrentino & Farrington, 2019), it seems legitimate to also ask the question - to what extent do the strategies used by teachers and other stakeholders in the school ecosystem consider the important psycho-pedagogical contexts associated with digital attacks on teachers? Answering this question, however, first requires mapping the current strategies and then locating them against the background of the processes that occur in the students' school and family environments.

Questions about the legitimacy of researching targeted attacks on teachers are related to several important processes occurring in the school ecosystem. First, attacks on teachers raise questions about the role and authority of the modern teacher in schools. Second, cyber-aggression and cyber-bullying that targets teaching staff not only by students but also by their parents generates concerns among teachers about the perception of the school ecosystem by all stakeholders. Third, the occurrence of this type of situation prompts reflection on the level of technical, administrative, and legal preparedness of teachers and school leaders to deal with this type of problematic situation, as well as the real level of protection offered to teachers. Fourth, research that includes teachers not as guarantors of digital security, but as potential victims changes the optics of the phenomena occurring in schools. Fifth, the proposed research is an attempt to respond to the needs of this socially important professional group, which in many countries is struggling with new phenomena for which it has not been prepared in its studies or lifelong learning (Chen & Cui, 2022; Pace, 2019).

Online attacks against teachers are characterized by different levels of harmfulness, may be carried out directly or indirectly, and may be characterized by full or partial visibility in the online space and therefore not always be directly perceptible to the person attacked. Responding appropriately to these forms of attack requires specialist knowledge and competence for the removal of harmful content. The increasingly sophisticated forms of online attacks targeting educators (including the use of artificial intelligence) also necessitate an update of solutions enabling legal protection for teachers (Kong et al., 2021). Knowing and understanding the mechanisms of protection against e-threats that are not sufficiently described in the literature is one of the first steps to empowering teachers both competently and psychosocially (McMahon et al., 2023).

RESEARCH METHODOLOGY

Aim and Subject of the Study

The aim of the research is to delineate the strategies for dealing with attacks on teachers that are carried out in cyberspace and that stem from their profession. The aim of the research is to fill an empirical gap in designing and carrying out activities aimed at the digital safety of teachers. The implementation of the research aligns with the need to create evidence-based solutions to strengthen teachers' digital competence. Therefore, the research has a scientific purpose, which is to create a typology of strategies for solving problematic situations faced by teachers in cyberspace and beyond. This analysis also has a practical purpose related to the presentation of specific solutions that can potentially be implemented through in-service training programs or the education of future generations of teaching staff.

The subject of this study is the statements of teachers who have experienced attacks in online spaces by students or the parents of students. The statements deal with difficult personal experiences and describe not only the nature of cyberbullying or cyberaggression (Tomczyk et al., 2024a) but, importantly, explore the approaches, techniques, solutions, and knowledge that made it possible to stop the attack or resolve the problematic situation.

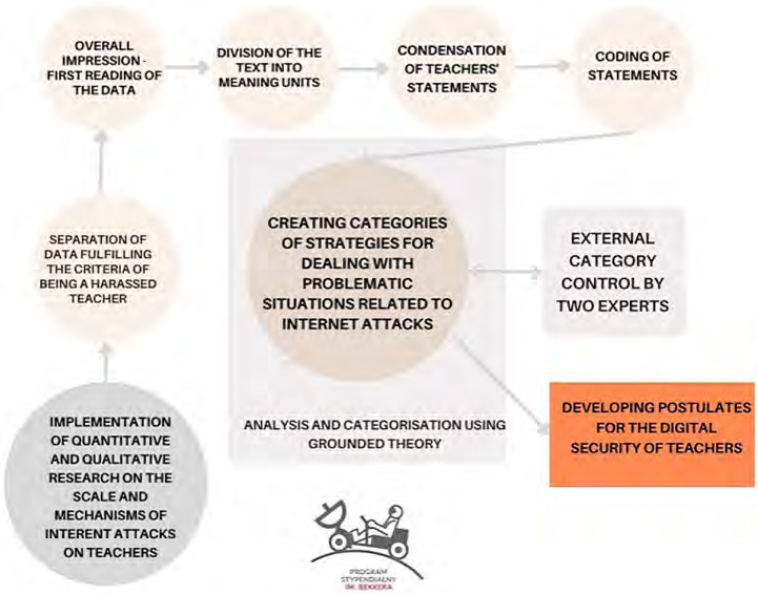

Figure 1. Research procedure to identify strategies for dealing with situations involving online attacks targeting teachers (Source: The author's own elaboration)

Test Procedure

The research was conducted in late 2023 and early 2024. The research was carried out with the support of the National Agency for Academic Exchange (NAWA), which funded a project entitled 'digitally safe teacher' (a national module of the Mieczyslaw Bekker Program). The target group was teachers who had experienced an online attack (cyber-aggression or cyber-bullying) because of their profession. Respondents participating in the study completed an anonymous online questionnaire about the extent of the phenomenon under analysis. This was followed by a separation of the data into two groups: teachers who had experienced any kind of attack from students and/or the parents of students; and those who had not experienced any kind of attack.

The data collected from in-service teachers who had experienced an online attack (N = 58) were subjected to a five-stage analysis according to the approach proposed by Graneheim and Lundman (2004). In the first stage, the entirety of the teachers' statements on their means of coping with online attacks were read several times in order to gain a general understanding and to determine the contexts of this complex situation. As a second step, the different means of dealing with this situation were extracted from the statements and divided into meaning units. In the third step, the statements selected were abbreviated with logicality without losing the characterization of interventions relating to addressing cyberbullying and cyberaggression. In the fourth step, the units of meaning were coded in order to describe in a synthetic way the strategies for addressing the problem. In the final step proposed by Graneheim and Lundman (2004), the codes that emerged in the fourth step were grouped on the basis of similarities and differences. The grouped codes were given consistent names for the categories of coping strategies for Internet attacks. The extracted codes were externally validated (Johnson, 1997) by two experts working on the issue of cyberbullying and electronic aggression (IH > 20, at least 10 publications indexed in the Scopus database on the topic of the Internet risk behavior). Based on the interpretation of the categories by the external experts, the names of the categories were corrected, and research limitations were added to the resulting typology. The entire empirical part was also the basis for the development of postulates for pedagogical practice enhancing teachers' digital safety. The research process is shown in **Figure 1**.

The data analysis was carried out using principles derived from grounded theory due to the inductive approach to the creation of new theories (typologies of strategies), developed from the personal experiences of teachers who were attacked online. The use of solutions anchored in grounded theory also allowed for an iterative and distributed data collection process, providing the possibility for an adaptive and flexible approach to the creation of typologies (Chiovitti & Piran, 2003; Prigol & Behrens, 2019). This approach stems from the specificity of the research subject, which is changing with the development of new e-services, the

Figure 2. Strategies for dealing with problematic situations related to online attacks (Source: Prepared by the author with MS Copilot)

style of use of ICT among young people, the reshaping of models of digital competence, and the changing awareness of digital safety among teachers.

Research Ethics

In keeping with the nature of the research problem, the data collection process was completely anonymous. The research did not process any data that would enable the identification of the interviewees and therefore the attribution of problematic situations (the Internet attacks) to specific individuals. The participating teachers were informed about the scientific purpose of the research, the ways in which their stories would be processed and presented, and the possibility of opting out of the research procedure and withdrawing their own statements at any stage. The activities were carried out according to the procedure of sensitive biographical research methodology (Surmiak, 2022). The design, collection, and processing of the data were carried out in accordance with the Declaration of Helsinki and were also approved by NAWA (BPN/BKK/2022/1/00007/DEC/1).

FINDINGS

On the basis of the analyses carried out and the categorization of the responses according to the model proposed by Graneheim and Lundman (2004), nine strategies reported by the respondents were delineated. These strategies are differentiated according to level of restrictiveness, intra-institutional responsibility, type of external support, and level of autonomy of action carried out by teachers. A list of ways to deal with situations involving an ICT attack on a teacher because of their profession is presented in **Figure 2**.

Student-Oriented Education and Prevention Activities

Addressing an attack in the online space is done through typical educational activities. For this purpose, many teachers use instructive and activation methods that aim to make their students aware of the consequences of actions that violate good morals, and of the legal protection of public officials such as educators. It should also be noted, referring to R222's statement, that the formation of the ability to understand the consequences as well as the impact of cyber-attacks is a tedious phenomenon from the perspective of achieving educational goals and often requires repetition on the part of the teaching staff.

> Explain to students the legal consequences of such behavior (R8, F, 26).

> It took almost a semester, a complex process, talks, workshops (R222, F, 45).

Educational activities in the school system can be carried out by both the teachers themselves and by external actors. Given the context of the research problem, i.e., actions that violate the good image of the teacher and violations of prevailing social and legal norms, external actors can be involved in solving this type of problem. The police can be listed among those with competence and knowledge related to cybercrimes

and juvenile delinquency. Some respondents (R52 and R121) have been assisted by external preventive support in the event of an attack.

> Discussions have taken place with children about the consequences of online activities, lack of anonymity, online safety, also with the participation of representatives from the police (R52, F, 35).

> The police were called in to talk to the students (R121, F, 40).

A specific form of workshop following an online attack against a teacher involves the students, who are obliged to prepare activities for their peers as part of repairing the harm done. This form of PBL offsets some of the inadequacies of previous solutions related to educational support provided by people outside the school ecosystem.

> Student-led activities in grades 4-8 on the topic of hate speech and the legal responsibility of the perpetrator if detected (R292, F, 47).

Given the very nature of the school as an institution whose aim is to shape the knowledge, skills, and attitudes of its students, it is logical that one of the basic pillars for solving problematic situations should be educational in nature. The forms mentioned by the respondents clearly indicate that educational and preventive measures (in the case of an attack situation, tertiary prevention) are particularly important for shaping basic knowledge among students about the consequences of the actions they take, both in the online and offline spaces.

Working With the Student's Family

The previous category clearly outlines the role of educational and upbringing activities aimed at the student perpetrator of cyberbullying. The next category extends the palette of educational activities to the students' families. The responses presented below delineate a complementary type of action aimed at raising awareness of the mechanisms and consequences of an online attack. This category is particularly relevant due to the inclusion of those responsible for the activities undertaken by young people outside of the school environment in the remediation process, with a concomitant impact on activities occurring in school settings.

> A meeting was held for parents on online hate. Measures were taken to resolve the problem causing the heist between parents (R51, F, 35).

> A meeting on the situation was held between the parents of the students, the headmaster, and the teacher (R86, F, 38).

> Parents were called to the school, interviews with students in the presence of a psychologist, educator, principal (R102, F, 39).

> We held discussions with students and their parents. We organized workshops for the students and lectures for the parents (R630, M, 58).

Interventions among parents include not only educational activities, but also the presentation of recommendations related to a restrictive media parenting model. The statement of R140 clearly suggests that removing the problematic situation requires strengthening parental control over the activities that young people undertake on the Internet.

> The teacher invited the parents of the students to a meeting where he presented the problem and asked for educational interventions and increased parental control over what the children do on the Internet (R140, F, 42).

This category related to parental pedagogy takes on a new meaning when cultural differences are considered. The example presented by R713 makes it clear that some attacks on teachers can result from a number of factors, requiring individual work with the whole family while considering broader contexts that go beyond the mechanisms of a typical Internet attack.

> This was an online comment from a Ukrainian student not accepting the situation he was in; explanatory discussions were held with the mother and the student with the help of a Ukrainian-speaking teacher, the incident has not recurred, the student is not causing trouble (R713, M, 61).

Undoubtedly, the role of the school is to strengthen digital safety for all stakeholders. This task requires, in the first instance, working with the offender and, in the case of minors, the use of activities that involve the students' family. This category is an exemplification of the primary role of the school, which is the psychoeducation of both students and the students' parents.

Removal of Harmful Content From the Internet

Attacks on teachers require a variety of educational as well as technical measures. Teachers who are victims of slander, or who are exposed to disparaging material about themselves on websites, newsgroups, and social networks, emphasize the need to remove such harmful content efficiently and quickly.

> Content has been reported to the operator and blocked (R208, F, 44).

> Blocking of the site and its updates by the administrator (R301, F, 47).

> With great reluctance, the administrator removed some of the information (R471, F, 53).

Referring to R30's statement, however, it is important to be aware that not all content can be completely eliminated due to the nature of the digital material that appears on the web. Despite the removal of material that damages the image of the teacher from the original place where it was posted in some situations, copies of any videos, memes, comments, and photos are easy to place in other repositories, websites, and instant messengers. Therefore, the removal of harmful content is not always a fully effective action.

> Some of the recordings were deleted, unfortunately some were permanently put on the Internet and can still be found today (R30, M, 31).

The implementation of actions triggering the procedure of deleting such content from the Internet requires, in the first instance, the monitoring of the Internet space or the occurrence of other circumstances in which the attacked teacher becomes aware of the situation.

> This was reported by a parent of another student, a conversation with the relevant parent resulted in the photo being removed from the Internet (R220, F, 45).

The specific nature of attacks on teachers requires actions similar to those taken in the case of peer-to-peer cyberbullying. One such activity is to secure a copy of the harmful material and then attempt to remove the content.

Teachers' Independent Activities

Some of the respondents act independently both in terms of identifying the perpetrator of the attack and removing the harmful content. The actions listed in the descriptions below clearly show that the lack of systemic support for teaching staff necessitates the ability to track down the attacker or, if possible, to block the source of the attack.

> The teachers surveyed established the identity of the students and actions were taken against him, including that he would change his entry (R57, M, 35).

> We have reached the creator of the profile. The profile has been terminated (R537, F, 55).

> The comment was hidden by the profile administrator at the request of the teacher (R132, F, 41).

Self-help actions carried out by teachers have clear objectives. First of all, those attacked want to remove content that portrays them in an unfavorable light and acts according to the 24/7/365 rule. The punishment

of the offender is very often linked to the implementation of different types of consequence depending on the scale of the breach of boundaries related to social norms.

> The group/someone was threatened with consequences and this group disappeared (R545, F, 55).

> Students removed the photo after discovering the fact and apologized to the teacher (R672, F, 60).

Self-action can also be forced through lack of external support, as evidenced by the case presented by R666. In that situation, the teacher relied on multifaceted actions including a change of perspective to bring the unwanted action to a halt. In the case of R666, it was clearly important to the respondent not only to stop the attack, but also to bring closure to the issue in a way that allowed for the triggering of student empathy.

> The headmaster did not want to deal with the matter ex officio. I myself fought to organize an assembly with the students and told them my feelings. This resulted in a conversation between the author and his mother. The boy explained that he wanted to show off in front of his friends and apologized to me (R666, M, 59).

Some attacks on teachers require the cooperation of the victim or a team of educators to track down the perpetrator and remove the content. The examples cited by R279 and R723 clearly suggest that individual resolution of a problematic situation is not always possible without the support of others in the school ecosystem.

> Students found out who shared the access code to the teacher's profile and informed the teacher (R279, F, 46).

> The case was resolved by a team of teacher educators (R723, F, 65).

Individual teacher action is among the first to be taken. However, the effectiveness of individual action is conditioned by the level of digital and media competence, as well as human relations capital and the characteristics of the school in which the educator works. Individual actions are a kind of litmus test showing the true level of skills in dealing with crisis situations at the interface between online and offline spaces.

Notifying the Police

Teachers who become victims of attacks are not always able to remove harmful content on their own and to find the perpetrator. Therefore, in extreme cases, i.e., situations where they feel physically threatened or the attacks are long-term, some respondents choose to notify law enforcement. However, as evidenced by the statements of R294 and R650, the police are not always able to find the perpetrator.

> The teacher lodged a notice with the police. Perpetrators acquitted (R14, F, 26).

> Reported to police, person responsible for entries not found (R294, F, 47).

> Report of the incident to the police. After many months the case was dropped, the perpetrator was not discovered (R650, F, 59).

> Case reported to the police (concerning the publication of an image without the teacher's consent) (R91, F, 38).

In some cases, notifying the police is not acceptable behavior in the school itself. The situation cited by R19 clearly indicates that the solution to a troublesome situation in many establishments is based only on internal strategies to deal with such problems, and that the external involvement of the police is not deemed as being acceptable.

> The case was laid out by the police and there was criticism from the management for trying to resolve the situation through the police (R19, F, 30).

The issue of teacher cooperation with the police appears twice in this section. In the first case, it is of an educational nature, while in the second case it is related to the search for help in discovering the perpetrator and the search for possible assistance. In the second case, teachers do not always (in their perspective) receive due assistance, which may be due to the complexity of the technical aspects of attacks on teachers.

Involvement of Judicial Authorities

The statements in the previous category are linked to another group of actions taken by the respondents. Teachers who are victims of an attack such as blackmail, threats, or permanent vilification first seek help from law enforcement agencies. When the perpetrator of such actions is discovered, some of the respondents decide to notify the authorities to determine pathological situations in the child's household.

> After reporting to the police, the student appeared in court (R167, F, 43).
>
> I reported the harassment to the police. The case ended up in court (R285, F, 47).
>
> Such actions may not only take on a typically criminal dimension–prosecuted ex officio–but may also be taken individually, e.g., when a teacher's good image has been damaged. The teacher went to civil court in this case (R69, F, 36)

The actions described can result in consequences for students. In the case of R254, the teachers' attempt to enforce justice was not completed to the satisfaction of the aggrieved party. In contrast, R477 and R719, based on their own experiences, emphasize the effectiveness of the judiciary and the application of punishments appropriate to the acts committed.

> The case ended up in court, unfortunately the students were acquitted (R254, F, 46).
>
> There was a hearing before the juvenile court, the student had to apologize to the teacher on social media and in person (R477, F, 53).
>
> The case happened many years ago, the student was punished by the juvenile court, he was placed under the care of a probation officer (R719, F, 64).

Intervention by both law enforcement and judicial institutions (civil action, criminal action, family court) is a strategy that requires the collection of evidence for the case and usually results from a significant violation of social norms. This type of category is not a situation that teachers resort to very often, which can be explained by consideration of the complexity of legal processes and the need to incur costs.

Individual Consequences for the Student Resulting From the School's Internal Regulations

The issue of consequences for students is regulated not only in the framework of judicial actions mentioned in the previous category, i.e., the penal code and the family code, or civil law, but also at the school level. Some educational institutions have precise regulations regarding the consequences that an attack on a teacher on the Internet may have. Typically, such an action may result in a reduction of the student's grade for behavior, suspension from school, or an intensive corrective action involving the primary environment of the offender.

> Drawing the consequences provided for in the school's statutes against the student (R163, F, 43).
>
> Students were held accountable (reprimanded) (R164, F, 43).
>
> Principal's reprimand, withdrawal of student rights for a specified period, reprimanded behavior for a semester, discussions with parents (R255, F, 46).
>
> The student was punished in accordance with the penalties provided for in the school's statutes (R236, F, 45).

The individual consequences for the student resulting from the school's internal regulations is a type of strategy that is put in place before an attack on a teacher occurs. Internal regulations clearly set the boundaries between acceptable behavior and behavior that violates digital safety. However, it is important to be aware that not all school establishments have documents of this kind, or that these regulations are necessarily visible to the students themselves.

Combining Different Forms of Interaction

Crisis situations force teachers to undertake different activities simultaneously. This may be due to the specifics of the attack on the teacher, the need to remove destructive material from the Internet, and the development of mechanisms to block the recurrence of undesirable behavior. In the examples below, it is apparent that a poor grade for behavior or a public reprimand is combined with other restrictive actions. The solutions proposed by R8, R67, R23, and R606 are intended to highlight the negative consequences of the actions taken by the students.

> Tracking of perpetrators by the management, reduction of the grade for behavior of the students responsible, meeting with police officers on cyberbullying for the class where the situation took place (R8, F, 26).

> Conversations with parents, consequence of reduced grade for behavior (R67, F, 36).

> Interview with the student and their parents in the presence of the head teacher and school counsellor. Bring to the attention of the student with negative points for behavior and removal of the photo/video from all places where the photo/video was published (R23, F, 31).

> The student was reprimanded in front of the class and has a reduced grade for behavior. His parents took away his mobile phone (R606, F, 57).

In the case of a serious breach of norms, the solutions mentioned earlier (disciplinary action on school premises) are taken, as well as the involvement of external bodies such as the police. This multi-faceted action sends a clear signal to the whole school community that the behavior is not only subject to local consequences, but also has repercussions beyond the school.

> The case is developing, the police are investigating, and the school has also taken disciplinary action (R72, M, 37).

> Teacher (and other students) informed of situation. Case reported to the teacher and procedure launched, who took the photo, where was it published. In addition, the parents of the students informed, confronted and the case reported to the police (R176, F, 43).

Another type of dual response is combining dialogue-based activities with blocking harmful content. Dialogic methods can be carried out both at the teacher-student level as well as with the wider community in mind, thus including parents as well as the entire teaching community.

> The website was quickly removed and those responsible had discussions with this teacher, who was their tutor (R41, F, 34).

> The matter came to light very quickly (thanks to information from one of the students involved in the case), the account was immediately deleted, the students admitted their guilt and apologized. Discussions were held with them and their parents (R130, F, 41).

> Blocking the ability to comment, training council for the whole board of education (R438, F, 52).

In the context of a two-tier impact, the full involvement of parents in explaining the situation, as well as the establishment of the rules and consequences resulting from a cyber-attack targeting a teacher, plays an important role in the process. The responses presented below clearly suggest that this overlap is aimed at

establishing the boundaries of acceptable behavior with the simultaneous involvement of parents, whose aim is to participate in the process of correcting the behavior.

> Report to the principal, discussion with support–psychological-educational counselling center, parents, note for diary (R252, F, 46).

> Parents were summoned and threatened by the court to review the family situation for possible pathologies. This helped, the content was removed (R312, F, 48).

> The student's tutor and parents were informed of the case. An explanatory interview was held with the student's parents and the student herself. She was informed about the possible consequences of publishing online statements with elements of vulgarity referring, for example, to teachers or classmates (R331, F, 48).

Combining the different forms reinforces the educational impact with a sense of forewarning – any actions undertaken by potential perpetrators should already come with a clear idea of the consequences. This approach, however, requires the appropriate selection of these strategies, which is not an easy task and is linked to external support in the form of family and tertiary prevention organizations.

No Response

Among the strategies for dealing with attacks on teachers, a ninth complementary category emerged, under which teachers noted inaction as a form of response. Their silence in the situation may be due to a sense of anonymity, e.g., hurtful posts, or not treating the analyzed situations as threatening to the teacher in any way.

> The school did not take personal action as the entry was anonymous. There were positive posts under the entry from other parents (R65, F, 36).

> There was no official discussion of the matter (R197, F, 44).

The lack of response may be intentional. According to R286 and R17, there are situations where those with a real say in resolving such crisis events do not interact as desired. Inaction here can be considered an attempt to resolve the situation by waiting for it to simply go away.

> None. Nothing has been done. No support, complete. Everyone wanted the subject to be over quickly (R286, F, 47).

> It was not reported - it quietened down after some time (R17, M, 28).

In the statements of R400 and R428, a perspective of non-responsiveness is evident, which is combined with a feeling of bitterness. Both respondents point out that teachers do not receive the real support that they should receive from, among others, school management. In addition, R400 adds that punishments for students may be inadequate in nature.

> The principal swept the matter under the carpet. The principal didn't even move the student to another class. I had to watch him for 8 months, pretending nothing happened. Everyone was watching my every move, whether I was sometimes taking revenge on the student (R400, F, 51).

> He was ignored by the principal. Teachers are left alone with such problems (R428, F, 51).

An interesting perspective on attacks on teachers is presented by R10, who emphasizes that non-response can be intentional, but at the same time should be linked to knowledge of the mechanisms of the attacks on teachers. Non-reaction may be an adequate response to some forms of attacks that do not represent a viable threat to the relevant teacher.

> In none and that is a good thing. Until teachers know the attack procedure there is nothing to worry about. I have had students experience more than once–attempts at recording, etc. But you have to know what and there is is no problem (R10, M, 27).

As presented in this section, non-responsiveness can take different appearances. A lack of response in some cases may be an intentional and acceptable action, while in another it may be an indicator of an inefficient support system for teachers who are victims of an attack. The lack of response is a category that needs to be placed in a broader context, considering digital security policies, or the real preparation of school leaders to support teachers at risk of attack from students and/or the students' parents.

DISCUSSION

The data collected clearly suggest that teachers who are attacked on the Internet due to their profession have an extensive palette of protective possibilities, which stem from their own educational and digital competences, as well as the resources of the local environment and legal solutions. These approaches show how many possibilities a modern teacher has to react through, from a soft-educational response to the situation, through the involvement of parents and external institutions in the process of stopping cyberbullying, to restrictive solutions (the police and the court). Among the respondents' statements, a 'strategy' of silence and lack of appropriate response also emerges, which clearly demonstrates the need for a discussion on teacher safety in the modern school and the need for solutions to increase the protection afforded to teachers (Berkowitz et al., 2022; Gregory et al., 2012; López et al., 2020). The strategies presented are the cumulative knowledge of teachers, which can be used directly in a threatening situation or serve as a basis for prevention. The collected and systematized data from the empirical part can also become the basis for designing school strategies in a hypothetical situation of an attack on teaching staff. At the same time, it is worth emphasizing that strategies of this kind are rare and that the topic of teachers' digital security is still insufficiently researched and does not have an adequate translation into preventive measures (Tomczyk et al., 2024b).

The protection strategies presented serve not only to solve the problematic situation from the perspective of the teacher–the victim of the digital attack–but also encourage the formation of elementary knowledge of legal responsibility among students and parents. Such an assumption is particularly evident in terms of activities such as educational and preventive workshops aimed at students or the involvement of the student's family in the correctional process. In these two categories, the educational-preventive mission of the school is clearly visible (Greenberg, 2010; Miller et al., 2005), the aim being to create effective solutions to enhance knowledge about safety (including digital issues). Such activities can be carried out not only using the assumptions of primary prevention, but also secondary and tertiary prevention (Cichosz & Tyburska, 2014; Gaś, 2006; Pospiszyl, 2008). This approach explicitly assumes that the attack on the teacher is the starting point for workshop activities, lectures, and meetings with external experts that build media awareness as well as digital competence in both the perpetrators and their victims (Sonck et al., 2014). In the two categories indicated, there is a shift away from a restrictive approach to acting with the clear objective of increasing knowledge and understanding of the consequences of inappropriate ICT use. Knowledge and skills in and about the secure use of ICT are now becoming an integral part of digital competence. A lack of skill in this area, as shown in the empirical section decreases the feeling of digital safety, increasing vulnerability to attacks from students or parents.

Among the responses analyzed, two further categories of activity are also of interest, the removal of harmful content from the Internet, and the teachers' own activities. Both activities firstly require having information about the attack, i.e., where the harmful content is located, as well as how the harmful content is being disseminated. This knowledge is directly linked to digital skills (Chou & Sun, 2017) related to securing data, searching for information, being able to communicate with e-service administrators to remove harmful content, and tracking down the creators of such content (Bilbao Aiastui et al., 2021; Chou & Peng, 2011). Self-action and attempts to remove harmful content are therefore based on fundamental digital competences relating to the area of digital security. The ability and knowledge to protect oneself is a useful acquisition not only in the perspective of one's profession, but also in everyday life. However, given the scale of potential losses (e.g., reputational, emotional, and financial) associated with the profession, there is now a need to

strengthen teachers' digital competences anchored not only in the paradigm of opportunities (e.g., effective support of teaching processes), but also in the paradigm of risks (e.g., prevention of behaviors classified as cyberbullying and cyberaggression).

Furthermore, it is important to note that the digital competence component in question can serve to counteract behavior that is not only directed at teachers themselves, but also at students who become helpless in the event of ICT-mediated peer violence.

Each type of cyber-attack on a teacher is characterized by a different course, form, impact, and legal consequence. Among the statements identified, there is also an approach related to the legal consequences in the case of an attack on a teacher. In such a situation, a selected group of people refers to actions related to reporting the incident to the police and involving law enforcement authorities. Such an approach may be due to the attacker overstepping boundaries, where the teacher feels genuinely threatened, or other means of influence have failed. The implementation of solutions based on legislation is a process that does not always conclude in accordance with the perceptions that teachers bring to the situation. The effectiveness of law enforcement agencies related to the discovery of the perpetrators of attacks on teachers, as well as court judgements, do not always satisfy the victim. The actions assigned to the two categories indicated are an interesting point to discuss the level of legal protection of teachers (Suharyanta, 2020; Zahuri & Israhadi, 2021), which should complement the previously mentioned categories.

The two categories based on legislation are partly linked to the consequences for students in the dimension of the school ecosystem. Regulations related to digital safety in this case are established not only through general societal norms (Piccoli et al., 2020; Young & Tully, 2019), but school documents that make clear what behaviors are not acceptable and what consequences are sure to follow (Beckstrom, 2008; Marczak & Coyne, 2010). Local-level regulations for a micro-community such as a school build a sense of security, set clear boundaries, and provide a reference point for regulating behavior at school. However, it is important to note that arrangements of this kind are not found in all school settings, which differentiates the level of safety of school ecosystems. There is also a need for further research into the awareness of support for those responsible for the management of establishments with regard to digital security, including the resolution of situations described in the empirical section. Currently, research of this kind is rare in situating research on digital safety of teachers under attack by parents and teachers in the area of empirical and theoretical gaps.

Among the categories here, there is the interesting area of combining different action strategies. The triangulation of different forms of influence is related to several objectives:

(1) protecting oneself from the negative impact of harmful content,

(2) removing harmful content,

(3) tracking down the perpetrators of the action,

(4) drawing consequences, and

(5) shaping appropriate competences among the perpetrators of the event.

Taking multifaceted action requires the possession of appropriate digital and media competences, as well as pedagogical intuition related to the selection of appropriate content, methods, and forms of educational work. This category also shows the diversity of actions that the teacher-victim must take in order to constructively resolve the situation (Cox et al., 2017; Espelage, 2017; Tomczyk et al., 2024a). The triangulation of strategies may also be due to the fact that the attacked teachers often face different forms of attack, which in turn requires non-standard-multi-track-action. Removing the cause of the attack, which is inherent in the school environment, requires, e.g., removing harmful material, setting boundaries and legal consequences for the attackers, as well as taking educational measures. The triangulation of strategies is therefore justified by the specifics of the teaching profession and is also necessitated by the circumstances, i.e., the form of the attack and its consequences.

Among the categories identified, the complete absence of a reaction to a teacher attack deserves special attention. The lack of reaction may be intentional on the part of the teacher or due to the attitude of the environment in which the event took place. The intentional lack of reaction may be due to the specifics of the attack, which the teacher may classify subjectively as non-threatening and not requiring educational intervention or be due to a lack of procedures being in place. The second dimension of the situation that has

arisen appears to be a doubly problematic situation. The victim teacher is placed in an emotionally and socially disadvantageous situation and, in addition, is not protected by procedures or environmental support. Situations of this kind need to be considered on an individual basis in each case of an attack on a teacher and should also consider the level of preparedness of school management and school supervisors to provide the necessary assistance. The lack of response in many cases for teachers expecting any action is an additional stressor.

Research Limitations and New Research Directions

The research results presented are an attempt to map the strategies that are employed when an attack on a teacher occurs. The nine strategies listed allow us to present the basic actions that are taken in schools when teacher-student relationships are violated. The listed forms of attack, due to the qualitative nature of the research, do not present the scale of actions taken, and are in many cases separated from the characteristics (including the causes) of attacks on teachers. The presented forms of action in a crisis situation also do not present the wider context, such as, for example, the climate of the school, the quality of the relationship between the teacher and student, or the forms of support for teachers by school management. The presented research results are difficult to compare with similar research results from Poland or neighboring countries due to the lack of interest of media educators in the indicated topics. The inability to relate the typology created here to other examples makes it impossible to show longitudinal changes in the forms of teachers' reactions to becoming a victim. The research limitations are also related to the impossibility of relating the strategies used to the level of media and digital competence of the teachers involved, which requires further (quantitative) research. Therefore, given the aforementioned research limitations, it seems reasonable to conduct further analyses showing the variation of coping strategies occurring in relation to previous experiences of cyberbullying and cyberaggression, and style and proficiency of ICT use, as well as the variation of strategies due to sociodemographic variables (age, gender, amount of experience in education, type of school, and level of potential support in the school environment).

CONCLUSIONS

This article is an attempt to present teacher strategies related to addressing cyberbullying and cyberaggression. The topics presented in this article have so far not been sufficiently explored or subsequently transferred to the professional education of future and current teachers (Tomczyk & Fedeli, 2022). Although the digitization of education is a rapidly progressing phenomenon (Szyszka et al., 2022), contemporary schooling has not always kept up with the positive and negative consequences brought about by the intensive use of ICT by students and their parents (Gabarda Méndez et al., 2021). The transformations taking place in education through new media force an in-depth reflection not only on the process of implementing ICT in didactics, but also on the preparation and support of teachers to respond to negative developments.

The nine teacher-focused strategies for addressing digital attacks presented here are not only an attempt to present ways to address such challenges, but more importantly to engage in (or trigger) a discussion on the need to strengthen digital security among students and across the entire school ecosystem (Karabatak & Karabatak, 2018; Zakia & Yana, 2023). Given the irreversible changes that digitalization is bringing about in many areas of human life, as well as the need to strengthen teachers' key competences, this study can also serve in shaping procedures for addressing such challenges in contemporary education.

Funding: This article is a part of the project funded by the NAWA under the Mieczyslaw Bekker Program.

Ethics declaration: This study was approved by NAWA (BPN/BKK/2022/1/00007/DEC/1). This study was conducted in accordance with the Declaration of Helsinki. Written informed consents were obtained from the participants.

Declaration of interest: The author declares no competing interest.

Data availability: Data generated or analyzed during this study are available from the author on request.

REFERENCES

Arifin, S. (2020). Challenges for teacher profession in contemporary Indonesia: A regulatory analysis. *Lentera Hukum, 7*(2), 117–136. https://doi.org/10.19184/ejlh.v7i2.17718

Beckstrom, D. C. (2008). State legislation mandating school cyberbullying policies and the potential threat to students' free speech rights. *Vermont Law Review, 33*, 283–321.

Berkowitz, R., Bar-on, N., Tzafrir, S., & Enosh, G. (2022). Teachers' safety and workplace victimization: A socioecological analysis of teachers' perspective. *Journal of School Violence, 21*(4), 397–412. https://doi.org/10.1080/15388220.2022.2105857

Bilbao Aiastui, E., Arruti Gómez, A., & Carballedo Morillo, R. (2021). A systematic literature review about the level of digital competences defined by DigCompEdu in higher education. *Aula Abierta, 50*(4), 841–850. https://doi.org/10.17811/rifie.50.4.2021.841-850

Bjelajac, Ž., Filipović, A. M., & Stošić, L. V. (2022). Internet addiction disorder (IAD) as a consequence of the expansion of information technologies. *International Journal of Cognitive Research in Science, Engineering and Education, 10*(3), 155–165. https://doi.org/10.23947/2334-8496-2022-10-3-155-165

Bo, M., & Onwubuya, G. C. (2022). The role of legislation in K-12 school discipline: The silence of action. *Frontiers in Psychology, 13*. https://doi.org/10.3389/fpsyg.2022.916925

Bostancı Bozbayındır, G. (2019). Cyberbullying and criminal law. *İstanbul Hukuk Mecmuası, 77*(1), 425–450. https://doi.org/10.26650/mecmua.2019.77.1.0009

Chen, F., & Cui, X. (2022). Teaching controversial issues online: Exploring college professors' risk appraisals and coping strategies in the US. *Teaching and Teacher Education, 115*, Article 103728. https://doi.org/10.1016/j.tate.2022.103728

Chiovitti, R. F., & Piran, N. (2003). Rigour and grounded theory research. *Journal of Advanced Nursing, 44*(4), 427–435. https://doi.org/10.1046/j.0309-2402.2003.02822.x

Chou, C., & Peng, H. (2011). Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience. *The Internet and Higher Education, 14*(1), 44–53. https://doi.org/10.1016/j.iheduc.2010.03.006

Chou, H. L., & Sun, J. C. Y. (2017). The moderating roles of gender and social norms on the relationship between protection motivation and risky online behavior among in-service teachers. *Computers & Education, 112*, 83–96. https://doi.org/10.1016/j.compedu.2017.05.003

Cichosz, W., & Tyburska, A. (2014). Profilaktyka agresji i przemocy w środowisku rodzinnym i szkolnym [Prevention of aggression and violence in the family and school environment]. *Studia Gdańskie*, (35), 93–110.

Cox, T., Marczak, M., Teoh, K., & Hassard, J. (2017). New directions in intervention: Cyber-bullying, schools and teachers. In T. M. McIntyre, S. E. McIntyre, & D. J. Francis (Eds.), *Educator stress: An occupational health perspective* (pp. 411–435). Springer. https://doi.org/10.1007/978-3-319-53053-6_17

Espelage, D. L., & Hong, J. S. (2017). Cyberbullying prevention and intervention efforts: Current knowledge and future directions. *The Canadian Journal of Psychiatry, 62*(6), 374–380. https://doi.org/10.1177/0706743716684793

Fredrick, S. S., Coyle, S., & King, J. (2022). Middle and high school teachers' perceptions of cyberbullying prevention and digital citizenship. *Psychology in the Schools, 60*(6), 1958–1978. https://doi.org/10.1002/pits.22844

Gabarda Méndez, V., García Tort, E., Ferrando Rodríguez, M. de L., & Chiappe Laverde, A. (2021). Pre-school and primary school teachers: Technological training and digital competence. *International Journal of Technology and Educational Innovation, 7*(2), 19–31. https://doi.org/10.24310/innoeduca.2021.v7i2.12261

Gaś, Z. B. (2006). *Profilaktyka w szkole* [Prevention at school]. WSiP.

Graneheim, U. H., & Lundman, B. (2004). Qualitative content analysis in nursing research: Concepts, procedures and measures to achieve trustworthiness. *Nurse Education Today, 24*(2), 105–112. https://doi.org/10.1016/j.nedt.2003.10.001

Greenberg, M. T. (2010). School-based prevention: Current status and future challenges. *Effective Education, 2*(1), 27–52. https://doi.org/10.1080/19415531003616862

Gregory, A., Cornell, D., & Fan, X. (2012). Teacher safety and authoritative school climate in high schools. *American Journal of Education, 118*(4), 401–425. https://doi.org/10.1086/666362

Jaskulska, S., Jankowiak, B., Pérez-Martínez, V., Pyżalski, J., Sanz-Barbero, B., Bowes, N., Claire, K. D., Neves, S., Topa, J., Silva, E., Mocanu, V., Gena Dascalu, C., & Vives-Cases, C. (2022). Bullying and cyberbullying victimization and associated factors among adolescents in six European countries. *Sustainability, 14*(21), Article 14063. https://doi.org/10.3390/su142114063

Johnson, R. B. (1997). Examining the validity structure of qualitative research. *Education, 118*(2), 282–292.

Karabatak, S., & Karabatak, M. (2018). Teachers' knowledge levels about virtual information security. In *Proceedings of the 6th International Symposium on Digital Forensic and Security* (pp. 1–5). IEEE. https://doi.org/10.1109/isdfs.2018.8355330

Kong, Z., Xue, J., Wang, Y., Huang, L., Niu, Z., & Li, F. (2021). A survey on adversarial attack in the age of artificial intelligence. *Wireless Communications and Mobile Computing, 2021*(1), Article 4907754. https://doi.org/10.1155/2021/4907754

Kopecký, K., & Szotkowski, R. (2017). Specifics of cyberbullying of teachers in Czech schools–A national research. *Informatics in Education, 16*(1), 103–119. https://doi.org/10.15388/infedu.2017.06

López, V., Benbenishty, R., Astor, R. A., Ascorra, P., & González, L. (2020). Teachers victimizing students: Contributions of student-to-teacher victimization, peer victimization, school safety, and school climate in Chile. *American Journal of Orthopsychiatry, 90*(4), 432–444. https://doi.org/10.1037/ort0000445

Macaulay, P. J. R., Betts, L. R., Stiller, J., & Kellezi, B. (2018). Perceptions and responses towards cyberbullying: A systematic review of teachers in the education system. *Aggression and Violent Behavior, 43*, 1–12. https://doi.org/10.1016/j.avb.2018.08.004

Marczak, M., & Coyne, I. (2010). Cyberbullying at school: Good practice and legal aspects in the United Kingdom. *Journal of Psychologists and Counsellors in Schools, 20*(2), 182–193. https://doi.org/10.1375/ajgc.20.2.182

Marín-López, I., & Zych, I. (2024). Bullying, cyberbullying, and social, emotional, and moral competencies. In A. L. C. Fung (Ed.), *Cyber and face-to-face aggression and bullying among children and adolescents: New perspectives, prevention and intervention in schools* (pp. 72–87). Routledge. https://doi.org/10.4324/9781003414933-7

Mascia, M. L., Agus, M., Zanetti, M. A., Pedditzi, M. L., Rollo, D., Lasio, M., & Penna, M. P. (2021). Moral disengagement, empathy, and cybervictim's representation as predictive factors of cyberbullying among Italian adolescents. *International Journal of Environmental Research and Public Health, 18*(3), Article 1266. https://doi.org/10.3390/ijerph18031266

McMahon, S. D., Bare, K. M., Cafaro, C. L., Zinter, K. E., Garcia-Murillo, Y., Lynch, G., McMahon, K. M., Espelage, D. L., Reddy, L. A., Anderman, E. M., & Subotnik, R. (2023). Understanding parent aggression directed against teachers: A school climate framework. *Learning Environments Research, 26*(3), 915–931. https://doi.org/10.1007/s10984-023-09460-2

Mihailidis, P., Shresthova, S., & Fromm, M. (2021). *Transformative media pedagogies*. Routledge. https://doi.org/10.4324/9781003031246

Miller, T. W., Kraus, R. F., & Veltkamp, L. J. (2005). Character education as a prevention strategy in school-related violence. *Journal of Primary Prevention, 26*, 455–466. https://doi.org/10.1007/s10935-005-0004-x

Oksanen, A., Celuch, M., Latikka, R., Oksa, R., & Savela, N. (2021). Hate and harassment in academia: The rising concern of the online environment. *Higher Education, 84*(3), 541–567. https://doi.org/10.1007/s10734-021-00787-4

Pace, J. L. (2019). Contained risk-taking: Preparing preservice teachers to teach controversial issues in three countries. *Theory & Research in Social Education, 47*(2), 228–260. https://doi.org/10.1080/00933104.2019.1595240

Pennell, D., Campbell, M., Tangen, D., & Knott, A. (2021). Should Australia have a law against cyberbullying? Problematising the murky legal environment of cyberbullying from perspectives within schools. *The Australian Educational Researcher, 49*(4), 827–844. https://doi.org/10.1007/s13384-021-00452-w

Pfaffinger, K. F., Reif, J. A. M., Spieß, E., & Berger, R. (2020). Anxiety in a digitalised work environment. *Gruppe. Interaktion. Organisation. Zeitschrift Für Angewandte Organisationspsychologie (GIO), 51*(1), 25–35. https://doi.org/10.1007/s11612-020-00502-4

Piccoli, V., Carnaghi, A., Grassi, M., Stragà, M., & Bianchi, M. (2020). Cyberbullying through the lens of social influence: Predicting cyberbullying perpetration from perceived peer-norm, cyberspace regulations and ingroup processes. *Computers in Human Behavior, 102*, 260–273. https://doi.org/10.1016/j.chb.2019.09.001

Pospiszyl, I. (2008). *Patologie społeczne. Resocjalizacja* [Social pathologies. Resocialization]. PWN.

Prigol, E. L., & Behrens, M. A. (2019). Grounded theory: Methodology applied in education research. *Educação & Realidade, 44*(3), Article e84611. https://doi.org/10.1590/2175-623684611

Pyżalski, J., Plichta, P., Szuster, A., & Barlińska, J. (2022). Cyberbullying characteristics and prevention–What can we learn from narratives provided by adolescents and their teachers? *International Journal of Environmental Research and Public Health, 19*(18), Article 11589. https://doi.org/10.3390/ijerph191811589

Rajbhandari, J., & Rana, K. (2022). Cyberbullying on social media: An analysis of teachers' unheard voices and coping strategies in Nepal. *International Journal of Bullying Prevention, 5*(2), 95–107. https://doi.org/10.1007/s42380-022-00121-1

Romero Rodrigo, M., Gabarda Méndez, C., Cívico Ariza, A., & Cuevas Monzonís, N. (2021). Families at the crossroads of media and information literacy. *International Journal of Technology and Educational Innovation, 7*(2), 46–58. https://doi.org/10.24310/innoeduca.2021.v7i2.12404

Saladino, V., Eleuteri, S., Verrastro, V., & Petruccelli, F. (2020). Perception of cyberbullying in adolescence: A brief evaluation among Italian students. *Frontiers in Psychology, 11*. https://doi.org/10.3389/fpsyg.2020.607225

Sanders, C. E. (2022). *Cyberbullying: Definition, prevalence, risk factors, consequences, and prevention*. Routledge. https://doi.org/10.4324/9780367198459-reprw25-1

Schimmel, D., & Militello, M. (2007). Legal literacy for teachers: A neglected responsibility. *Harvard Educational Review, 77*(3), 257–284. https://doi.org/10.17763/haer.77.3.842n787555138746

Šimandl, V., & Vaníček, J. (2017). Influences on ICT teachers knowledge and routines in a technical e-safety context. *Telematics and Informatics, 34*(8), 1488–1502. https://doi.org/10.1016/j.tele.2017.06.012

Sonck, N., & de Haan, J. (2014). Safety by literacy? Rethinking the role of digital skills in improving online safety. In S. van der Hof, B. van den Berg, & B. Schermer (Eds.), *Minding minors wandering the Web: Regulating online child safety* (pp. 89–104). TMC Asser Press. https://doi.org/10.1007/978-94-6265-005-3_5

Sorrentino, A. & Farrington, D. (2019). Individual, family, peer, and school risk factors for teacher victimization. *Educational Sciences: Theory & Practice, 19*(4), 1–13. https://doi.org/10.12738/estp.2019.4.001

Suharyanta, S. (2020). Implementation of legal protection for teachers to tackling criminal acts of persecution. *MAGISTRA Law Review, 1*(2), 94–102. https://doi.org/10.35973/malrev.v1i2.1613

Surmiak, A. (2022). *Etyka badań jakościowych w praktyce* [Ethics of qualitative research in practice]. Wydawnictwo Naukowe Scholar.

Szyszka, M., Tomczyk, Ł., & Kochanowicz, A. M. (2022). Digitalisation of schools from the perspective of teachers' opinions and experiences: The frequency of ICT use in education, attitudes towards new media, and support from management. *Sustainability, 14*(14), Article 8339. https://doi.org/10.3390/su14148339

Thompson, R. (2021). Teachers and cyberbullying: Interventions, workarounds and frustrations. *Asia-Pacific Journal of Teacher Education, 50*(2), 187–201. https://doi.org/10.1080/1359866x.2021.1895967

Tomczyk, Ł. (2023). *New media pedagogy: Research trends, methodological challenges and successful implementations*. Springer. https://doi.org/10.1007/978-3-031-44581-1

Tomczyk, Ł. (2024). Digital competence among pre-service teachers: A global perspective on curriculum change as viewed by experts from 33 countries. *Evaluation and Program Planning, 105*, Article 102449. https://doi.org/10.1016/j.evalprogplan.2024.102449

Tomczyk, Ł., Fedeli, L. (2022). *Digital literacy for teachers*. Springer. https://doi.org/10.1007/978-981-19-1738-7

Tomczyk, Ł., Guillén-Gámez, F. D., Llorent, V. (2024a). Teacher digital and media competence in cyber security–A perspective on individual resilience to online attacks. In Ł. Tomczyk (Ed.), *New media pedagogy: Research trends, methodological challenges, and successful implementations. NMP 2023. Communications in computer and information science* (pp. 1–23). Springer. https://doi.org/10.1007/978-3-031-63235-8_1

Tomczyk, Ł., Guillén-Gámez, F. D., Mascia, M. L., & Llorent, V. J. (2024b). How are teachers being attacked online? On cyberbullying and cyberaggression that targets school educators from the student's perspective. *Online Journal of Communication and Media Technologies, 14*(3), Article e202431. https://doi.org/10.30935/ojcmt/14602

Torres-Hernández, N., & Gallego-Arrufat, M. J. (2022). Indicators to assess preservice teachers' digital competence in security: A systematic review. *Education and Information Technologies, 27*(6), 8583–8602. https://doi.org/10.1007/s10639-022-10978-w

Young, R., & Tully, M. (2019). 'Nobody wants the parents involved': Social norms in parent and adolescent responses to cyberbullying. *Journal of Youth Studies, 22*(6), 856–872. https://doi.org/10.1080/13676261.2018.1546838

Zahuri, D., & Israhadi, E. (2021). Juridic review of legal protection towards teachers as educators. In *Proceedings of the 1st International Conference on Law, Social Science, Economics, and Education*. https://doi.org/10.4108/eai.6-3-2021.2306193

Zakia, R., & Yana, D. (2023). English teachers' perception of security in digital literacy competence. *Journal on Education, 5*(3), 8873–8882. https://doi.org/10.31004/joe.v5i3.1685

Zăvoianu, E.-A., & Sun, K. (2022). Can teachers be victims of cyberbullying? *Technium Social Sciences Journal, 33*, 92–97. https://doi.org/10.47577/tssj.v33i1.6843