



GRZEGORZ ŚWIECARZ

WSGE University of Applied Sciences
in Józefów, Poland

ORCID iD: 0000-0001-9007-0907

CYBERBULLYING AGAINST CHILDREN AND ADOLESCENTS – LEGAL FRAMEWORK AND PREVENTIVE STRATEGIES

ABSTRACT

In the era of widespread digitisation, childhood and adolescence take place in an environment strongly saturated with information technology, which – apart from its developmental potential – carries a number of threats to the psychological and social safety of the youngest users. One of the most serious phenomena of a destructive nature is cyberbullying – a form of psychological violence carried out through electronic media. The aim of this article is to analyse the phenomenon of cyberbullying among children and adolescents in the context of the current legal regulations in force in Poland and selected preventive actions taken by educational institutions. Particular attention was paid to the undefined status of cyberbullying in the legislative system, an analysis of the provisions of the Penal Code and the regulations stemming from the Act on Counteracting the Threat of Sexual Offences. The model of juvenile responsibility and the educational and correctional function of contemporary re-socialisation measures are also presented. The article demonstrates the need for an integrated approach to cyberbullying prevention, encompassing both legal tools and educational, relational and environmental measures with the common goal of protecting children from digital victimisation and supporting them in building a safe online identity.

KEYWORDS: *cyberbullying, children and young people, electronic violence, juvenile responsibility, legal protection, prevention, digital education, regulation*

INTRODUCTION

Children and adolescents grow up in a digital environment strongly shaped by information and communication technologies. Digital media influence not only communication and education, but also identity formation and emotional functioning. Despite their benefits, digital technologies also generate significant risks for children and adolescents. One of the most significant threats is cyberbullying. The scale of this phenomenon and its serious psychological and social consequences make cyberbullying appear as one of the most significant challenges for the child and adolescent mental health system, but also for the educational system, the family and the law.

Increasingly, dramatic accounts of children and adolescents experiencing online bullying are making their way into the public eye, setting off a wave of public concern and questions about the effectiveness of existing protection and intervention mechanisms. In particular, statistics published by the World Health Organisation (WHO) Regional Office for Europe are alarming, showing that as many as 15% of school-age young people have

experienced cyberbullying personally, while 12% admit to using it against peers (See also: UNESCO, 2020). The phenomenon is not only spreading, but also shows gender differences – statistically, boys are more often the perpetrators (14%) than girls (9%). The situation in Poland is particularly noteworthy, with as many as 26% of 15-year-old boys admitting to online violence and 18% of 13-year-old girls (Report on Peer Violence, 2024). These alarming proportions indicate not only the growing scale of the problem, but also the need to analyse it in depth and develop multi-level response strategies – both at the systemic level and at the local, family and school level.

This study aims at a multifaceted analysis of the problem of cyberbullying among children and adolescents from the perspective of legal solutions in force in Poland and preventive practices undertaken by educational and upbringing institutions. Particular emphasis will be placed on discussing the undefined status of cyberbullying in the national legislative system, which in practice hinders effective protection of underage victims and limits the possibility of unambiguous qualification of perpetrators' actions. The analysis will also take into account the role of the school as an upbringing-preventive environment, the tasks of institutions supporting the development of children and young people, as well as the importance of parental awareness and education in terms of safe functioning in virtual space. The presented considerations lead to the conclusion that effective prevention and counteraction of cyberbullying requires not only legal interventions, but also a change in social mentality, strengthening the educational competence of adults and supporting children in building healthy and responsible relations in the digital world.

CYBERBULLYING – DEFINITIONS AND TYPOLOGIES OF THE PHENOMENON

From the perspective of further analysis, it becomes indispensable to define precisely the essence of the phenomenon of cyberbullying, whose interdisciplinary nature and dynamic development force constant updating of definitions and typologies. Cyberbullying is a form of psychological and social violence conducted through digital technologies. E. Smerecka (2016) defines cyberbullying as a repetitive, hostile action by an individual or group

(referred to as cyberbullies), directed against the victim (cyberoutsider) and carried out through a variety of digital channels – such as websites, discussion forums, social media, instant messaging, email, webcams, fake profiles, game consoles, texting or phone calls. In this view, the essence of the phenomenon is not only the intentionality of the action, but also the use of modern technological tools as a medium of aggression and psychosocial destabilisation of the victim (Abawajy, 2014).

Cyberbullying, although embedded in the classic mechanisms of interpersonal violence, exhibits distinctive features resulting from the digital reality – in particular the anonymity of the perpetrator, the possibility of immediate dissemination of content and the potential indelibility of compromising material. Contemporary research indicates that this phenomenon not only intensifies the victim's sense of helplessness, but also blurs the boundaries between the real and virtual worlds, leading to real psychological consequences such as chronic stress, anxiety disorders, depression or suicidal thoughts (Siemieniecka-Gogolin et al., 2017).

In the context of further considerations, it is crucial to distinguish the various forms of cyberbullying, the identification of which enables more effective preventive and legal action (Aloul, 2012). Cyberbullying includes various forms such as harassment, humiliation, exclusion and dissemination of harmful content.

Particularly harmful are forms violating privacy and sexuality, such as non-consensual dissemination of intimate content. The group of violent activities also includes child grooming – which is the organised grooming of children by adults impersonating peers, with the aim of gaining trust and sexual exploitation, and phishing (spoofing), which refers to the phishing of personal information and identity theft for the purpose of gaining advantage or causing harm (Bandler, 2017).

The diversity of cyberbullying forms demonstrates the scale and complexity of this phenomenon, whose common denominator remains the psychological, emotional or social harming of another person using digital tools. The precise identification of the different types of cyberbullying is an essential starting point for the development of effective regulatory and preventive mechanisms to protect children and adolescents from its destructive consequences (Patchin & Hinduja, 2018).

CYBERBULLYING IN LEGAL REGULATIONS

When analysing the issue of cyberbullying in the context of the legal order in force in Poland, the fundamental issue remains the fact that this concept has not yet been unambiguously defined in normative acts. The lack of a separate, systematic definition of cyberbullying in legal regulations does not mean, however, that violent actions carried out through electronic media remain outside the scope of criminal responsibility. However, this dispersed regulation model should be assessed critically, as it does not ensure consistency in the qualification of cyberbullying behaviours. On the contrary, numerous acts falling within the scope of this phenomenon may be effectively prosecuted on the basis of the provisions contained in the current Penal Code, which, although it does not use terminology specific to the digital world, also includes within its scope those behaviours that are carried out with the use of communication technologies.

The first relevant group of provisions concerns offences against individual freedom. Of particular importance here is Article 190 §1 of the Penal Code, according to which a person threatening another with committing an offence to his or her detriment or to the detriment of a person close to him or her is subject to criminal liability to the extent that the threat arouses in the threatened person a well-founded fear of its realisation. In practice, this provision applies, *inter alia*, in situations where the perpetrator directs threats against the victim via electronic media – such as email, instant messaging or social networking sites – in a persistent and intimidating manner. If the recipient of such messages is a minor, in accordance with the provisions of the criminal procedure, the obligation to report the suspected offence lies with the minor's legal representative, who is most often a parent or legal guardian (Law of 6 June 1997, Article 190).

It is worth emphasising that the initiation of preparatory proceedings by law enforcement authorities follows the rules appropriate to this category of criminal offences, however – due to the specific situation of the victim – the actions taken require appropriate protective measures. One of the most important of these is the interrogation of a child in psychologically friendly conditions, the so-called *blue room*, in accordance with the principle of one-offness and with

the obligatory participation of an expert psychologist, whose task is to support the minor and ensure the proper course of evidentiary activities taking into account his/her age and level of emotional development. Such procedural solutions serve not only to protect the procedural interests of the child, but also to limit the potential secondary victimisation that the child could suffer in the course of criminal proceedings (Podlewska, 2009, p. 7).

Among the legal regulations relevant for counteracting cyberbullying, a special place is occupied by Article 190a of the Penal Code, which refers to the problem of persistent harassment – also known as stalking – and the unlawful use of another person's identity. This provision, although not directly referring to the phenomenon of cyberbullying as a whole, is one of the most important tools to protect an individual from violence carried out through electronic communication means. Its effectiveness in practice is limited by the difficulty of proving persistence and psychological impact, especially in cases involving minors. Pursuant to Article 190a §1 of the Penal Code, criminal liability is imposed on a person who, through repeated actions, arouses in another person a justified feeling of threat, humiliation, anguish or leads to an infringement of that person's privacy. In the digital environment, stalking can take a variety of forms, including persistent sending of harassing messages, commenting on the victim's online activity, publishing compromising content or systematically following and interfering with the victim's virtual life (Act of 6 June 1997, art. 190a).

This phenomenon, in the case of minors, is particularly destructive because in children and adolescents – who are in a period of intense emotional and identity development – digital bullying can lead to serious psychological consequences such as anxiety disorders, depression, sleep disorders, social withdrawal and sometimes suicidal thoughts and attempts. Thus, in the context of cyberbullying, stalking becomes not only a tool of psychological violence, but also a risk factor for the victim's mental health, especially in conditions of emotional immaturity and limited competence in dealing with violent situations.

The second form of prohibited act included in Article 190a §2 of the Penal Code is the so-called identity theft, which consists in the unlawful use of another person's personal data – such as name, image, telephone number or e-mail address – in order to impersonate that person and cause personal or

property damage. In the context of the increasing number of social interactions carried out online and the pervasiveness of social media, this type of crime is becoming increasingly important. False profiles created on the basis of the victim's personal data may be used, *inter alia*, to disseminate offensive, derogatory or discrediting content, as well as to commit fraud, extortion or manipulate interpersonal relations (Act of 6 June 1997, Art. 190a §2 of the Penal Code).

Both persistent harassment and identity theft belong to the category of offences prosecuted at the request of the victim, which means that criminal proceedings can only be initiated after the victim has formally reported the case. If the victim of the criminal act is a minor, the obligation is transferred to his/her legal representative – usually a parent or legal guardian – who is obliged to file a notice of suspicion. This construction is intended, on the one hand, to ensure respect for the autonomy of the individual in deciding whether to take legal action, and on the other hand, to guarantee protection in situations of violation of personal goods, privacy and mental and emotional integrity, especially when the victim is not fully capable of acting independently in the legal sphere. Article 190a of the Penal Code, although not exhaustive of the entire issue of violence in cyberspace, is an important legal tool for responding to forms of digital violence of a particularly severe nature (Law of 6 June 1997, Article 190a §2 of the Penal Code).

In the context of the analysis of the legal aspects related to cyberbullying, it is impossible to ignore the provisions relating to crimes against sexual freedom, which in the digital environment gain a new and extremely disturbing dimension, especially with regard to minors. Of particular importance in this regard is Article 191a of the Penal Code, which criminalises the unlawful recording of an image of a naked person during a sexual act or in intimate situations – in a manner contrary to the person's will, without his or her knowledge or consent, and with the use of violence, threats or deception. This provision is directly applicable to the phenomenon of sexting, which is increasingly taking the form of non-consensual dissemination of erotic material, thus constituting a manifestation of psycho-sexual violence carried out through digital channels (Law of 6 June 1997, Article 191a).

In the case of children and adolescents, such actions constitute a particularly serious violation of their personal and bodily integrity, resulting in severe

emotional disturbances, loss of a sense of security, shame, fear of stigmatisation and dramatic consequences in the sphere of social relations. They strip the individual of control over their self-image, intimacy and identity, sometimes leading to severe psychological crises, including depressive episodes, social withdrawal and even suicide attempts (Owens, Behun, Manning, & Reid, 2012).

Another key provision regulating the sexual exploitation of children in cyberspace is Article 202 of the Criminal Code, which refers to offences related to child pornography. This provision criminalises a wide range of acts – from the production, recording and storage to the dissemination, sharing and public presentation of pornographic content involving minors. In practice, this means that any form of recording, transmission or publication of material depicting persons under the age of 18 in a sexual context – regardless of the form (graphic, audiovisual or textual) – is subject to prosecution under criminal law. Importantly, these offences fall into the category of acts prosecuted *ex officio*, which means that criminal proceedings are initiated regardless of the will of the victim. In light of the applicable legislation, anyone who has knowledge of the occurrence of such an act – irrespective of his or her status or function – is obliged to immediately inform the relevant authorities, such as the police or the public prosecutor's office. The law enforcement authorities are then obliged to undertake procedural actions, including the initiation of pre-trial proceedings, the securing of evidence and the identification of the perpetrator (Act of 6 June 1997, art. 191a).

The introduction of the indicated provisions into the national legal order is one of the most significant steps towards ensuring real protection of children and adolescents from sexual violence, including in the virtual space. Articles 191a and 202 of the Penal Code not only have a penalising and preventive function, but also have an important educational and symbolic dimension, clearly signalling that violations of corporeality, dignity and personal boundaries – regardless of whether they take place in the real or digital world – are subject to an unequivocal and uncompromising legal response. Thus, they become an indispensable element of a child's rights protection system in a digitalised society, where the boundaries of privacy are constantly shifting and the risks associated with the sexualisation of digital space are becoming

more and more widespread and difficult to neutralise without the involvement of appropriate legislative and educational mechanisms.

Among the provisions aimed at countering cyberbullying and ensuring comprehensive protection of children and adolescents from violence of a sexual nature, Article 200a of the Criminal Code, which refers to the phenomenon known as child grooming, is of particular importance. This term refers to the grooming of a child by an adult via electronic communication means in order to prepare the ground for future sexual exploitation. The issue has become particularly topical in an era of widespread access to the Internet for children and young people and the increasing number of relationships established in digital space, in which the boundaries of privacy, security and parental control are becoming increasingly difficult to set and maintain (Law of 6 June 1997, Article 200a).

Pursuant to Article 200a §1 of the Penal Code, anyone who, by means of an ICT system or a telecommunication network, establishes contact with a minor under 15 years of age with the aim of leading him/her to sexual intercourse, undertaking another sexual act, presenting pornographic content or a meeting which could result in sexual exploitation, is liable to punishment. Significantly, the legislator decided to criminalise not only the act of exploitation itself, but also the intentional preparation for its realisation – the very initiation of contact of a seductive nature, regardless of whether it has a physical effect, constitutes grounds for criminal liability. The introduction of this regulation is an expression of the tightening of the state's penal policy in the area of protection of minors and emphasises the prophylactic dimension of criminal law as a tool to prevent crimes of particular gravity (Act of 6 June 1997, Article 200a §1 of the Criminal Code).

The phenomenon of child grooming is particularly dangerous because of its latent, manipulative nature. The perpetrators' actions often take the form of a long-term process of gaining the child's trust, building emotional dependence and systematically breaking down the child's natural protective barriers. Psychological manipulation and exploitation of the victim's emotional immaturity and lack of life experience mean that this process can remain invisible for a long time, both to the child himself and to those around him. In many cases, perpetrators avoid overtly criminal actions by

operating in the realm of ambiguous messages, suggestions and subtle forms of influence that make it difficult to clearly qualify as a criminal act – until there is a direct threat to the child's integrity.

The introduction of Article 200a to the Penal Code should be interpreted as a response to these challenges – as this provision allows law enforcement agencies to intervene at the early contact stage, before violent actions escalate. It thus constitutes an important preventive instrument aimed at protecting children from the most severe forms of sexual victimisation, carried out under conditions of apparent anonymity and difficult to grasp during digital interaction. In this sense, Article 200a has not only a sanctioning function, but also an educational and warning function, setting the boundaries of legal responsibility for behaviour that may have hitherto remained beyond the reach of the criminal system's response. As a modern provision, adapted to the challenges of the information society, it constitutes one of the pillars of protection for underage users of the Internet space who, not yet having mature self-defence mechanisms, require special attention from the State and its protective institutions (Law of 6 June 1997, Article 200a).

Another important category of offences that are applicable in the context of counteracting cyberbullying are offences against an individual's personal goods, i.e. offences against honour and human dignity. In the Polish Penal Code, this area is regulated within the framework of two basic provisions: Articles 212 and 216, which gain particular significance in the conditions of developed Internet communication. Indeed, in the digital age, the boundaries between acceptable criticism and violation of personal dignity are often blurred, which encourages abuse and escalation of violent behaviour, especially against young and emotionally vulnerable people.

Pursuant to Article 212 §1 of the Penal Code, the offence of defamation consists in slandering another person, a group of persons, an institution, a legal person or an organisational unit without legal personality of such conduct or properties as to bring them into disrepute in public opinion or to expose them to a loss of confidence necessary to fulfil a specific function, exercise a profession or carry out an activity. In the reality of cyberbullying, this provision is particularly applicable in situations where online users publish untrue, defamatory information about a specific person – most often

a student, teacher, peer or member of the school community – in a way that damages their reputation and public perception. This content, disseminated on social networks, forums, newsgroups or through private messaging, can lead to stigmatisation, isolation and significant difficulties in interpersonal relationships. Defamation then becomes not only a form of violation of the law, but also a source of acute emotional suffering, which – especially in young people – can have long-lasting effects on their sense of self-worth and social identity (Law of 6 June 1997, Article 212 §1 CC).

The regulation contained in Article 212 is supplemented by Article 216 of the Penal Code, which criminalises insult – understood as insulting another person in a manner detrimental to their dignity, while the provision also covers actions carried out through the media, including electronic media. In practice, this refers to situations in which the victim is publicly insulted, laughed at, ridiculed or humiliated by means of content of a vulgar, contemptuous or derisive nature. Unlike defamation, insult does not require the content to be untrue – it is sufficient that it is offensive in its form and intent. In cyberspace, this often manifests itself in the form of insulting comments, memes of a ridiculing nature, the sharing of videos portraying a person in a disparaging light or posting humiliating posts about him or her (Law of 6 June 1997, Article 216).

However, it is worth emphasising that both the offences of defamation and insult belong to the category of so-called private prosecution offences, which means that their prosecution does not take place *ex officio*, but requires procedural activity on the part of the victim. In practice, this means that a private indictment must be filed with the competent district court. This significantly limits their practical applicability in cases involving children, as it requires legal initiative from parents or guardians. If the victim of cyberbullying is a minor, this obligation lies with the minor's legal representative – usually a parent or legal guardian – who acts on behalf of the child by taking the appropriate formal steps. Although this procedure may seem complicated, it is a viable tool for the protection of personal dignity and honour in the conditions of the digital communication space, where these violations not infrequently take on forms that are particularly psychologically and socially acute (Podlewska, 2009, p. 5).

The introduction and consistent application of the indicated provisions not only serve as a legal response to behaviours violating personal rights, but also set limits to socially acceptable forms of expression on the Internet, shaping a culture of communication based on respect for the dignity of another human being. In this sense, Articles 212 and 216 of the Penal Code also have an educative and normative function, indicating unequivocally that freedom of expression cannot be an excuse for verbal violence and social exclusion of persons at risk of digital victimisation.

The last category of provisions of the Penal Code, whose significance in the context of cyberbullying cannot be overlooked, are the regulations pertaining to the so-called hate speech, contained in Article 256 and Article 257. Although their primary function does not directly refer to interpersonal violence in the classical sense, in the digital environment they gain particular significance as instruments of criminalisation of content characterised by discrimination, prejudice and hostility towards specific social groups. Cyberspace, which is by nature an open, fast and anonymous environment, has become a space particularly susceptible to the dissemination of messages motivated by national, ethnic, racial, religious or ideological hatred (Act of 6 June 1997, Articles 256-257).

Pursuant to Article 256 §1 of the Penal Code, criminal liability is imposed on anyone who publicly propagates a fascist or other totalitarian state system or incites hatred on the grounds of national, ethnic, racial, religious or irreligious differences. This provision therefore covers both content of an ideological nature and that which is intended to incite prejudice and social antagonism. This regulation is complemented by Article 257 of the Penal Code, which criminalises the public insulting of a person or a group of persons because of their national, ethnic, racial, religious or irreligious affiliation. Both provisions are particularly applicable in the case of acts of cyberbullying, where hatred motivated by differences in worldviews takes the form of insulting, ridiculing, inciting to violence or presenting content of a xenophobic and extremist nature (Act of 6 June 1997, Articles 256-257).

The contemporary activity of young people on the Internet, although it is a natural space for their socialisation and expression, is unfortunately also increasingly associated with participation – both passive and active – in the

dissemination of hate content. A particularly worrying phenomenon is the presence of children and young people as victims or perpetrators of hate speech, which is often due to a lack of legal awareness, insufficient educational support and emotional and developmental conditions. Early exposure to discriminatory or radicalising content, especially in the absence of an adequate response from the adult environment, can lead to internalisation of intolerant attitudes, assuming the role of perpetrator of verbal violence and building an identity based on exclusion of the Other.

In this context, the provisions of Articles 256 and 257 of the Penal Code fulfil not only a repressive function, allowing for a formal legal reaction against actions that violate the dignity and security of specific social groups, but also an educative and normative function. They set limits to freedom of expression, reminding us that the exercise of freedom of expression must not lead to the violation of the rights of others and, in particular, must not be a tool of symbolic violence and social exclusion. In view of the increase in the number of hate-motivated incidents online, the consistent application of these regulations becomes not only a challenge for law enforcement agencies, but also a task for the entire education system – both formal and informal – which should shape attitudes of openness, respect and responsibility for words in the digital environment.

LEGAL RESPONSIBILITY OF MINORS

The issue of the legal responsibility of juvenile perpetrators of cyberbullying finds its normative basis primarily in the Act of 9 June 2022 on the Support and Rehabilitation of Juveniles, which replaced the previous regulations contained in the Act on Proceedings in Juvenile Cases. This Act, which is an expression of a new approach to the issues of demoralisation and juvenile delinquency, is at the same time a response to the changing social conditions, including the increased importance of violence realised in the digital environment.

According to the provisions of the Act, as a general rule, a person under the age of 17 is not criminally liable under the Criminal Code. This means that penal measures characteristic of adults, such as a fine, restriction of liberty or imprisonment, cannot be applied to juvenile perpetrators of cyberbullying. Nevertheless, the legislator provides a different catalogue of legal measures

aimed at counteracting the deepening of demoralisation phenomena, shaping normative attitudes and supporting the upbringing and re-socialisation process. In this sense, the model of juvenile responsibility is based on the paradigm of upbringing rather than repression (Act of 6 June 1997, art. 256).

The law introduces the principle of individualisation and adequacy of the legal response, according to which the state intervention should be proportionate to the nature of the act, the scale of the social threat, while taking into account the age, the level of psycho-physical development and the educational needs of the minor. Structured in this way, the system allows the family court to choose the measure most appropriate to the situation of the particular offender, with the primary objective remaining not so much to punish as to prevent future recidivism and promote social reintegration.

The catalogue of educational measures that may be applied in the case of a juvenile perpetrator of cyberbullying includes, *inter alia*, a warning, an obligation to behave in a certain way (e.g. apologise to the victim, repair the damage caused), entrusting the supervision of the juvenile to the parents or legal guardian, establishing supervision by a probation officer or a social organisation carrying out educational activities. In more complex situations, when the measures taken so far do not produce the expected results, it is possible to refer the juvenile to a probation centre, an organisation conducting rehabilitation or therapeutic activities, and, in cases of the highest degree of demoralisation, to place the juvenile in a youth education centre, a district education centre or in a professional specialist foster family (Act of 6 June 1997, art. 256).

At the same time, it is worth emphasising that the application of the indicated measures is not of a penal nature, but serves to protect the social interest by constructively supporting the minor in the process of making him/her aware of the harmfulness of the actions undertaken, strengthening pro-social attitudes and preventing further victimisation. With regard to cyberbullying, such a model of responsibility assumes that the young offender is not treated as a criminal *sensu stricto*, but as a person in need of support, behavioural correction and developmental orientation. In this view, the legal response has an educative and corrective function, based on dialogue, environmental influence and the creation of conditions for the restoration of social relations. Thus, the Juvenile Support and Rehabilitation Act is an important pillar of modern legal policy towards children

and adolescents, taking into account the specificity of digital violence and the need to counteract its effects not only through control and sanction mechanisms, but also through systematic upbringing, educational and preventive measures.

PREVENTIVE ACTIONS AND RESPONSES TO CYBERBULLYING IN LEGISLATION

This legislative gap continues to affect the effectiveness of legal and institutional responses. The evolution of the approach to this phenomenon is a response to the growing awareness of the threats that digital violence poses to the psychological, social and emotional functioning of children and young people. With the intensification of the use of information technologies by minors, countering cyberbullying is becoming not only a legal challenge, but also a task for the educational system, which is obliged to shape a safe development environment.

One of the key pieces of legislation that contains regulations on the protection of children from abuse, including in the context of cyberbullying, is the Act of 13 May 2016 on Counteracting the Threat of Sexual Offences and the Protection of Minors. This law makes it mandatory for educational institutions to implement the so-called Standards for the Protection of Minors (SOM), which aim to ensure children's safety in all dimensions of their functioning – physical, mental and digital (Błaszczak, 2024). These standards presuppose the need for early recognition of signals indicating that the welfare of the child is at risk, as well as setting out specific procedures for dealing with situations where violence is disclosed, including violence carried out in the virtual space (Law of 13 May 2016).

Particularly noteworthy is Article 22c of the aforementioned Act, which imposes an obligation on schools, kindergartens and childcare facilities to develop rules for the use of devices with access to the Internet, to implement procedures to protect children from accessing harmful content and to indicate ways of intervention and support in the event of digital violence. This obligation includes not only drafting rules and policies, but also carrying out education and training activities and engaging with parents and professionals. This means that every educational institution has a duty to act systemically in the area of cyberbullying prevention, to actively monitor threats and to respond according to the child protection standards set. This approach also

implies the co-responsibility of principals, teachers, educators and leading bodies to build a digital environment based on the principles of safety, respect for dignity and protection of privacy (Law of 13 May 2016, Article 22c).

The document entitled *Standard for Online Safety of Educational Institutions*, developed by the Ministry of Digitisation as a response to the growing need to organise procedures for the digital safety of pupils and educational staff, is also important in the framework of preventive measures. This publication provides a comprehensive guide to the principles of countering technological and violent threats, taking into account both organisational issues (e.g. IT infrastructure management) and psychosocial issues (e.g. recognising symptoms of digital victimisation). The document emphasises the need to carry out regular prevention activities, organise interventions in cases of threats, develop digital competences of teachers and students, and strengthen cooperation between schools and parents and external actors such as NGOs or child protection services (Bochenek et al., 2018).

This standard explicitly treats digital safety as part of the systemic management of the organisation – not only in the technological aspect, but above all in the relational and educational aspect. In doing so, it emphasises the need for media education, the formation of an informed, reflective approach to the use of new media, as well as the implementation of procedures to ensure the effective protection of children from symbolic, psychological and sexual violence in the online environment (Koperna & Pieprzyk, 2023, pp. 153-154). Cybersecurity should also be understood as a preventive tool reducing the causes of digital violence, not only its consequences (Wielec, 2023).

Despite the lack of a formal definition of cyberbullying in Polish law, systemic legislative, educational and organisational activities clearly indicate the desire to cover this phenomenon with coherent, interdisciplinary protection. The existing legislation – including the Act on the Protection of Minors and departmental documents – performs not only a protective function, but also a preventive and educational one, creating a framework for effectively countering digital violence in the environment of children and adolescents. In this sense, cyberbullying ceases to be seen as an incidental problem and begins to be understood as a complex threat requiring a multifaceted response from educational, child-rearing and social institutions (Leeks, 2018, pp. 133-134).

CONCLUSIONS AND RECOMMENDATIONS IN THE PERSPECTIVE OF THE SAFETY SYSTEM FOR CHILDREN AND YOUNG PEOPLE IN THE DIGITAL ENVIRONMENT

The analysis indicates that current legal mechanisms are fragmented and require stronger integration with educational and preventive systems. The virtual space is becoming a place of escalation of violent actions, which – due to their scale, the anonymity of the perpetrators and the rapid rate of spread of content – require not only intervention at the individual level, but above all a systemic response. Cyberbullying should therefore be seen as a significant threat to the psychological, emotional and social safety of young technology users, embedded in the broader context of population and digital safety in the conditions of today's information society (Livingstone & Stoilova, 2021).

In light of the existing legal regulations and the growing number of cases of digital victimisation, it becomes reasonable to develop integrated, multi-level protection strategies that would combine the legislative, educational, psycho-preventive and technological component. A key role in this respect is played by educational institutions, which – according to the provisions of the Act on Counteracting the Threat of Sexual Offences – are obliged to implement standards for the protection of children, including in the context of their digital activity. However, this protection cannot be limited to formal measures only. It is necessary to equip schools with viable threat identification tools, response protocols and psychological support systems for victims and perpetrators of violence, as well as to make it mandatory to document and report incidents of cyberbullying as part of an institutional safety monitoring system.

In the recommended model for countering cyberbullying, a special role should be assigned to education and prevention, carried out both in the school and family environment. This requires increasing the digital competence of teachers and educators, as well as parents' awareness of the symptoms of digital victimisation and how to respond appropriately. It is also necessary to implement media education, empathetic communication and online conflict management programmes that prepare children and young people to function in the digital reality in an informed and responsible manner (Kowalski, Limber, & McCord, 2019).

It is also worth pointing out the need to expand national cyber-security strategies to include a component for the protection of children from peer and sexual violence in the digital environment. Cyberbullying, being not only a pedagogical problem but also a phenomenon that violates legal and social norms, should be included in the state's internal security policy as a factor that disrupts the psychosocial development of the young generation and a potential source of long-term social costs. For this reason, the development of national guidelines covering the responsibilities of leading authorities, educational institutions, intervention services and non-governmental organisations in preventing digital violence and supporting children affected by it is called for.

From the perspective of the safety system for children and adolescents, cyberbullying therefore appears as a complex phenomenon, requiring not only intervention and criminalisation measures, but above all a coherent and long-term digital protection policy. This implies the need to integrate legislative, educational and psychological actions within a unified prevention model in which each institution – school, family, local government, police, NGOs and digital media – plays a specific role. Only the interaction of these actors can guarantee the effective protection of minors from online violence, thus contributing to the construction of a safe environment for development, identity and social relations in a digital society.

The phenomenon of cyberbullying, although lacking a precise definition in the Polish legal system, is increasingly recognized as one of the key challenges for contemporary child and youth protection policy. An analysis of criminal law provisions, the Act on Supporting and Resocializing Juveniles, and regulations governing safety in educational institutions clearly points to the need to approach cyberbullying as a multidimensional issue—legal, psychological, social, and educational. Particularly important is the reinforcement of preventive measures implemented within the school environment, the development of media literacy education, and the enhancement of parenting and pedagogical competencies among adults, including both parents and teachers. Without such integration, legal measures alone remain insufficient to effectively counteract cyberbullying among minors.

REFERENCES

- Abawajy, J. (2014). User preference of cybersecurity awareness delivery methods. *Behaviour & Information Technology*, 33(3), 237–248. <https://doi.org/10.1080/0144929X.2012.708787>
- Aloul, F. A. (2012). The need for effective information security awareness. *Journal of Advanced Information Technology*, 3(3), 176–183. <https://doi.org/10.4304/jait.3.3.176-183>
- Bandler, J. (2017). *Cybersecurity for the home and office: The lawyer's guide to taking charge of your own information security* (1st ed.). American Bar Association.
- Błaszczak, A. (2024). Cyberprzemoc – realne zagrożenie wobec dzieci i młodzieży. Krótki przegląd wybranych programów interwencyjnych. *Annales Universitatis Mariae Curie-Skłodowska, Sectio J – Paedagogia-Psychologia*, 37(2), 81–92. <https://doi.org/10.17951/j.2024.37.2.81-92>
- Borkowska, A. (2019). *Cyberprzemoc. Włącz blokadę na nękanie. Poradnik dla rodziców*. NASK Państwowy Instytut Badawczy.
- Knol-Michałowska, K. (2012). Rola rodziny w interwencji i profilaktyce zagrożeń w Internecie. *Studia Edukacyjne* (23), 301–328.
- Koperna, P., & Pieprzyk, J. (2023). Świat wirtualny jako przestrzeń aktywności młodych ludzi w perspektywie uczniów oraz w opiniach ich rodziców i nauczycieli. W: M. Gajewski (red.), *Współczesne przestrzenie aktywności młodzieży* (s. 151–175). Wydawnictwo Scriptum. <https://doi.org/10.15633/8788363241940.07>
- Kowalski, R. M., Limber, S. P., & McCord, A. (2019). *A developmental approach to cyberbullying: Prevalence and protective factors*. *Aggression and Violent Behavior*, 45, 20–32. <https://doi.org/10.1016/j.avb.2018.02.009>
- Leksy, K. (2018). Zdominowani przez technologię informatyczno-komunikacyjną – o konsekwencjach naznaczenia cyfrowym dzieciństwem. *Chowanna*, (2), 119–140.
- Owens, E. W., Behun, R. J., Manning, J. C., & Reid, R. C. (2012). The impact of exposure to Internet pornography on adolescents: A review of the research. *Sexual Addiction & Compulsivity*, 19(1–2), 99–122. <https://doi.org/10.1080/10720162.2012.660431>
- Patchin, J. W., & Hinduja, S. (2018). *Cyberbullying: Identification, prevention, and response*. Cyberbullying Research Center.
- Siemieniecka-Gogolin, D., Skibińska, M., & Majewska, K. (2020). *Cyberagresja – zjawisko, skutki, zapobieganie*. Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika.
- Smerecka, E. (2016). Cyberbullying. Wirtualne narzędzie realnej przemocy. *Kultura – Media – Teologia*, 25(2), 71–80.
- Wielec, M. (Red.). (2023). *Cyberbezpieczeństwo na rzecz zapobiegania przyczynom przestępczości*. Warszawa: Instytut Wymiaru Sprawiedliwości.

ONLINE SOURCES

- Bochenek, M. et al. (2018). *Standard bezpieczeństwa online placówek oświatowych* [Online]. Fundacja Dajemy Dzieciom Siłę. Dostęp 12 lipca 2025, z https://cyberprofilaktyka.pl/publikacje/ost_Standard_bezpieczenstwa_online_placowek_owsiatowych.pdf

- Livingstone, S., & Stoilova, M. (2021). *The digital environment and children's well-being: A multinational review*. United Nations Children's Fund (UNICEF). <https://www.unicef.org/reports/digital-environment-and-childrens-well-being>
- Raport o przemocy rówieśniczej. (2024). [Online]. Uniwersytet Warszawski. Dostęp 12 lipca 2025, z <https://www.uw.edu.pl/raport-o-przemocy-rowiesniczej/>
- UNESCO. (2020). *Behind the numbers: Ending school violence and bullying*. United Nations Educational, Scientific and Cultural Organization. <https://unesdoc.unesco.org/ark:/48223/pf0000373746>

LEGAL ACTS

- Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz.U. 1997, nr 88, poz. 553.
- Ustawa z dnia 13 maja 2016 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich, Dz.U. 2024, poz. 1802.
- Ustawa z dnia 9 czerwca 2022 r. o wspieraniu i resocjalizacji nieletnich, Dz.U. 2022, poz. 1700.