SARA **L**aw **R**esearch **C**enter
International **J**ournal of **L**egal and **S**ocial **O**rder, https://www.ccdsara.ro/ijlso
ISSN 2821 – 4161 (Online), ISSN 2810-4188 (Print), ISSN-L 2810-4188
Nº. 1 (2025), pp. 1-18

CYBERBULLYING. THE ISSUE OF SECURITY IN THE ONLINE ENVIRONMENT IN THE AGE OF DIGITIZATION

C.-E. TOLBARU

Received 27.09.2025; accepted 05.12.2025
First online publication: 16.12.2025
DOI: https://doi.org/10.55516/ijlso.v5i1.278

Carmina-Elena TOLBARU
PhD. Associate Professor (Law)
National University of Science and Technology Politehnica Bucharest,
Faculty of Economic Sciences and Law (Romania)
E-mail: carmina.tolbaru@upb.ro
ORCID ID: https://orcid.org/0000-0002-1854-8352

Abstract

The paper addresses the phenomenon of cyberbullying as an emerging form of digital violence in the context of accelerating digitalization processes and the extensive use of information technologies. The analysis is carried out from an interdisciplinary perspective – psychological, sociological, legal and technological –, focusing on defining characteristics of online bullying (repetitiveness, anonymity, power imbalance) and its disproportionate impact on victims. The study investigates behavioral typologies, gender and age differences, as well as the relationship between cyberbullying and traditional forms of bullying.

From a legal point of view, the research highlights the gaps in the Romanian legislative framework, analyzing in parallel the European standards and the recent jurisprudence of the European Court of Human Rights (the cases Buturugă v. Romania, Volodina v. Russia, M.Ș.D. v. Romania). The findings show the need for an autonomous criminalization of cyberbullying, as well as the adaptation of criminal legislation and public policies to the new digital realities. In this regard, the paper formulates integrated reform proposals – legislative measures, educational and social programs, technological solutions based on artificial intelligence and inter-institutional cooperation mechanisms – with the aim of strengthening the protection of victims and reducing the incidence of the phenomenon.

The conclusion underlines the need for a coherent national and European approach, in which legal instruments are complemented by digital education,

social responsibility and the active involvement of online platforms in preventing and combating cyberbullying.

Key words: *cyberbullying, criminal law, digital violence, victim protection, public policies, ECHR cases.*

INTRODUCTION

The profound transformations brought about by digitalization in contemporary society have redefined the way we interact, communicate and expose ourselves online. With all the undeniable benefits, this technological expansion also generates a series of vulnerabilities, among which the phenomenon of cyberbullying stands out – an emerging form of violence that, due to its invasive, repetitive and often anonymous nature, raises serious problems of online security and protection of fundamental rights. In the specialized literature, cyberbullying is defined as an intentional and repeated behavior of psychological or social aggression, carried out through electronic means – social networks, instant messaging, forums, gaming platforms – and exploits the anonymity, speed and permanence of digital communication (*Ray, McDermott & Nicho, 2024; Patchin &Hinduja, 2006, pp. 148-169*). The COVID-19 pandemic has increased reliance on digital media, especially among children and adolescents, leading to a documented increase in online bullying (*Sorrentino et al., 2023, p. 3*). Unlike traditional bullying, cyberbullying is characterized by the public visibility of the abuse, the difficulty of escaping it even in private, and the considerable challenges it poses in terms of regulation, surveillance, and effective intervention.

This paper aims to investigate the manifestations, causes, effects and institutional responses to cyberbullying, especially among adolescents and young people, but also by extension among adults. The phenomenon is analyzed in the context of accelerated digitalization, the lack of explicit criminal regulations and the difficulty of identifying aggressors in the online space.

The aim of the approach is to understand how the defining elements of cyberbullying – repetitiveness, power imbalance, anonymity – manifest themselves in various digital environments, as well as how they affect victims and create normative gaps. The following research questions are formulated:

- What are the main forms and typologies of cyberbullying in the contemporary online environment?

- How do age, gender and digital environment influence the incidence of cyberbullying?

- What legislative, technical and educational instruments can effectively contribute to preventing and combating this phenomenon?

The research is qualitative and interdisciplinary, being carried out through documentary analysis and review of international scientific literature; analysis of normative content regarding European and Romanian regulations in criminal

matters and data protection; case studies of the jurisprudence of the European Court of Human Rights (ECHR – Buturugă v. Romania, Volodina v. Russia, M.Ș.D. v. Romania); comparative analysis between traditional and cyberbullying forms.

A clear identification of the distinctive features of cyberbullying compared to traditional bullying is expected, as well as a systematization of digital behavioral typologies. It is estimated that a legislative vacuum will be highlighted in Romanian criminal law regarding cyberbullying and an integrated approach of technological, legislative and educational intervention is proposed.

The relevance of the topic is amplified by the increasing incidence of the phenomenon, including in Romania, as well as by the need to align the legal framework with current digital realities.

I. CONCEPTUAL DELIMITATIONS AND THEORETICAL FRAMEWORK

I.1. Definition and characteristics of cyberbullying

Cyberbullying is a relatively recent concept, emerging as an extension of traditional bullying, in the context of digitalization and expanded access to information and communication technologies (ICT). In classical literature, bullying is defined by three fundamental features – intentionality, repetition, and an imbalance of power (*Olweus, 1999, p. 9*). This definition remains a cornerstone and has been further elaborated in recent research, which adapts it to the digital context and to cyberbullying (*Menesini & Salmivalli, 2017, pp. 240–253; Sorrentino et al., 2023*). These features have been taken over and adapted in defining aggressive behaviors in the online environment.

In the literature, cyberbullying is described as "any aggressive, intentional, and repeated behavior involving the use of digital technologies by an individual or group to harm another individual who cannot easily defend themselves" (*Patchin & Hinduja, 2006, pp. 148-169*). Unfortunately, from a legal perspective, in many legal systems, cyberbullying is not clearly regulated, often subsumed under the general notions of harassment, defamation, threats, or invasion of privacy.

I.2. Related terms and concepts - online aggression, digital violence, cyberstalking

Specialized studies propose a series of related terms that outline different facets of aggression in the digital environment, through the prism of the complexity and diversity of forms of manifestation. Thus:

- Online aggression designates a hostile behavior carried out via the Internet, without necessarily assuming repetitiveness or imbalance of power (*Pornari & Wood, 2010, p. 82*).

- Digital violence is a broader concept, which includes harassment, threats, distribution without consent of personal or intimate information, deepfakes and forms of online exploitation (*Citron, 2014, pp. 67-73*).

- Cyberstalking involves the continuous monitoring of a person's activity in the online environment, for the purpose of intimidation, abusive surveillance or threat (*Weekes, Storey & Pina, 2025*).

Although, most of the time, these terms are used as synonyms, from an analytical point of view, it is important to notice the differences between them, as they have relevant connotations for understanding victimization mechanisms and for outlining appropriate institutional responses.

II. TYPES AND MANIFESTATIONS OF CYBERBULLYING

II.1. Diversity of forms of digital aggression

Cyberbullying encompasses a broad range of manifestations that continuously evolve alongside technological advancements and the diversification of digital communication platforms. Recent studies indicate that the intensive use of social networks, instant messaging applications, and online gaming environments is closely associated with the emergence of new forms of aggression that transcend the boundaries of traditional bullying (*Kowalski et al., 2014, pp. 1075–1077; Huang et al. 2021, pp. 3–4*).

These behaviors are often amplified by the characteristics of the digital environment, such as anonymity, the rapidity of content distribution, the lack of spatiotemporal boundaries, and the difficulty in identifying the perpetrators (*Slonje, Smith & Frisén, 2012, pp. 26-32*). The digital environment therefore favors a form of persistent harassment, difficult to interrupt, which can occur at any time of the day, without the victim being able to retreat to a safe space (*Smith, 2012, p. 95*).

II.2. Behavioral typologies

The literature identifies a wide range of behaviors associated with cyberbullying. “Online aggression” is defined as those hostile actions carried out via the Internet or messaging, which do not necessarily involve repetition or power imbalance (*Pornari &Wood, 2010, pp. 81-94*). Cyberstalking is analyzed as a form of invasive digital monitoring in personal relationships, where partners obsessively monitor the victim’s online activity, for the purpose of intimidation or control. These practices are included in the broader concept of interpersonal electronic surveillance and are highlighted as real digital violence in recent studies (*Montero-Fernández, López-Sebastián & Del Moral-Pascual, 2023*). Among the most frequently reported forms of cyberbullying are:

- intentional exclusion of a person from a group or message thread;
- repeated sending of hostile messages;
- online impersonation and the publication of false or compromising content;
- the dissemination of intimate information without consent;
- the distribution of sexual images without the person's consent;

- as well as behaviors specific to the gaming environment, such as ”griefing”.

In the specialized literature there are proposals for a typology of aggressive motivations in the school and online context, distinctions between rage, revenge, reward and recreation, which can anticipate the roles of aggressor and/or victim (Runions et al., 2018). Therefore, there is a great diversity of cyberbullying manifestations, which can be identified and investigated by reference to the media used (mobile phones, internet), to the more specific ways of using ICT (text messages, instant messaging, email, web pages, etc.), as well as by the type of behavior. These categories offer a useful perspective in the in-depth understanding of the typologies, the digital context in which they occur and the motivations of the aggressors is essential for identifying effective prevention and intervention strategies.

II.3. Age and gender differences

One of the most important vulnerability factors in cyberbullying is age. Adolescents and preadolescents are particularly exposed, both as potential victims and as aggressors, as this stage of development involves intensive use of technology and increased sensitivity to social validation *(Kowalski et al., 2014, pp. 1083–1085*). Also, emotional self-regulation and risk assessment capacities are being formed, which contributes to impulsive decisions and heightened reactions to online attacks.

Longitudinal studies suggest that involvement in cyberbullying behaviors occurs at increasingly younger ages and may continue into adolescence and early adulthood, but with a lower frequency (*Ševciková & Šmahel, 2009, pp. 227–229*). Thus, age becomes both a predictor and a differentiating element in the intensity and form of manifestation of the phenomenon.

Gender is another significant determinant of cyberbullying. There is empirical evidence that indicates a gender-specific distribution of aggressive behaviors, both as victims and as aggressors. In general, boys are more likely to engage in direct, visible forms of aggression (e.g., name-calling, threats), while girls more frequently engage in subtle or relational forms, such as exclusion, rumor-spreading, and social manipulation (*Slonje & Smith, 2008, p. 150; Smith, 2012, pp. 95-96*).

In terms of cyberbullying, girls are often more likely to engage in indirect, social media-specific forms, such as denigrating through posts or sharing personal content without consent (*Livingstone & Görzig, 2014, pp. 10-11*). On the other hand, boys are more likely to engage in trolling or flaming, especially in contexts such as online video games (*Thacker & Griffiths, 2012, pp. 21-23)*.

However, these gender differences are not always uniform. Some recent research shows that the roles of victim and aggressor can alternate and be influenced by contextual factors, such as peer pressure, anonymity, social network

dynamics, and the degree of parental supervision (*Estévez et al., 2020, pp. 2-3, 15*).

II.4. Psychosocial factors

Beyond age and gender, a number of psychosocial factors contribute to an increased risk of victimization or involvement in online aggressive behaviors. These include:

• low empathy, which limits the aggressor's ability to understand the impact of his actions on the victim;

• moral disengagement, which allows aggressors to justify their behaviors (*Pornari & Wood, 2010, pp. 82- 83*);

• social isolation or lack of support from peers or family;

• poor parental supervision or lack of digital literacy;

• exposure to violent or aggressive content, which can normalize abusive behavior.

In a large systematic review, high empathy, active parental mediation, and a positive school climate are significant protective factors against cyberbullying (*Kasturiratna et al., 2024*). Similarly, research indicates that high levels of affective empathy are associated with a reduced likelihood of becoming a bully, but also with increased coping capacity among victims of cyberbullying (*Monteiro, 2024, p. 621*).

II.5. The influence of the digital environment

Technology plays an ambivalent role: on the one hand, it offers opportunities for communication, learning and expression, but on the other hand, it exposes users to risks and forms of aggression that are difficult to control. Online platforms not only allow the transmission of hostile messages, but also amplify them through viralization mechanisms, algorithms that reward controversial content and the lack of effective moderation measures (*Kowalski et al., 2014, pp. 1075–1077, 1080–1083*). In addition, anonymity and lack of supervision favor uninhibited behaviors that are less likely in face-to-face interactions. Thus, the online environment becomes not just a simple channel of communication, but a framework that shapes social behavior, often in the absence of clear norms or accountability (*Slonje, Smith & Frisén, 2012, p. 27*).

III. THE EFFECTS OF DIGITAL VICTIMIZATION

III.1. The psychological dimension of impact

Cyberbullying has a profound impact on the mental health of victims, often more severe than traditional forms of bullying. The most commonly reported psychological consequences include: anxiety, depression, shame, social withdrawal, anger, sleep disturbances, low self-esteem and, in extreme cases, suicidal ideation (*Hay, Meldrum & Mann, 2010, pp. 148-151; Kowalski et al., 2014, pp. 1090–1093*).

Unlike offline aggression, cyberbullying involves continuous exposure: the victim can be followed 24/7 by phone, social networks, email or other electronic means. Thus, the lack of a "safe haven" accentuates emotional suffering and creates a constant state of vulnerability (*Slonje, Smith & Frisén, 2012, pp. 26-32*).

Also, the anonymity of the aggressors and the difficulty of controlling the dissemination of information online lead to a loss of control over one's own image and personal identity. Offensive photos, comments or rumors can spread quickly, with the potential to reach a wide audience, which accentuates the public humiliation and stigmatization of the victim (*Citron, 2014, pp. 3-9, 23-27; Smith, 2012, pp. 95-96).*

III.2. Behavioral and social effects

Behaviorally, victims may develop avoidance of online environments, withdrawal from social activities, school absenteeism, decreased academic performance, and in some cases, aggressive reactions as a form of defense or counterattack (*Patchin & Hinduja, 2006, pp. 155-158, 160-161; Kowalski et al., 2014, pp. 1090–1093*). In certain situations, the victim may also become the aggressor, in a mechanism for transforming suffering into violence (*Kowalski et al., 2014, p. 1092*). At the same time, there is a distancing from family and friends, a lack of trust in adults, and a reluctance to report abuse — for fear of reprisals, mistrust, or ridicule (*Slonje, Smith & Frisén, 2012, pp. 29-30*). This institutionalized silence means that many cases of harassment remain unreported and untreated.

III.3. Overlap with and differences from traditional bullying

Unlike traditional forms of violence, cyberbullying is carried out through technology and online platforms, with distinct characteristics that increase its complexity and impact. Although cyberbullying and traditional bullying share a number of characteristics (intention to harm, power imbalance, repetitiveness), the differences between them significantly influence the intensity of the impact.

To differentiate cyberbullying from traditional bullying, seven specific characteristics have been identified in the specialized literature (*Smith, 2012, pp. 93-103*):

(1) it depends on a certain degree of technological expertise;

(2) it is a form of indirect manifestation, conferring anonymity;

(3) the perpetrator does not usually see the victim's reaction, at least in the short term;

(4) the complex role of the observer in cyberbullying - the viewer can be with the perpetrator when an act is sent or posted; with the victim when it is received; or none, when receiving the message or when visiting the respective website;

(5) traditional bullying is perpetrated through the status acquired by the perpetrator by demonstrating (abusive) power over others in front of witnesses, which is not applicable to cyberbullying;

(6) cyberbullying can reach high audience levels, unlike the audience involved in traditional bullying;

(7) the lack of a safe haven in cyberbullying – no matter where they are, the victim can be sent messages on their mobile phone or computer or they can access harmful information on social networks.

The distinctive features of cyberbullying — extended visibility, lack of physical contact, anonymity and virality — can lead to a much higher level of psychological distress, especially among adolescents. Thus, unlike classic bullying, cyberbullying incidents usually occur over longer periods than traditional bullying incidents.

Furthermore, the lack of immediate emotional feedback—often present in face-to-face bullying—reduces the possibility of empathy or remorse on the part of the aggressor, which makes the abuse easily perpetuated (*Slonje, Smith & Frisén, 2012, p. 27*).

IV. COPING STRATEGIES AND PREVENTION/INTERVENTION MEASURES

IV.1. Individual coping strategies

Victims of cyberbullying use a wide range of strategies, from simple technical measures – blocking the aggressor, deleting or reporting content, changing privacy settings – to direct responses to the aggressor. Studies show that avoidance and technological self-protection are the most common, but social support (family, friends, teachers) and the development of emotional regulation skills have a significant protective effect (*Hellfeldt, López & Andershed, 2020, pp. 12-14*).

IV.2. Educational and psychosocial interventions

Prevention programs based on digital education, introduced as early as primary school, reduce both victimization and aggressive online behaviors. Recent meta-analyses confirm the effectiveness of anti-bullying programs that include modules dedicated to the digital environment, especially when they actively involve students, parents and teachers (*Polanin et al., 2022, pp. 449-450*). Last but not least, awareness campaigns, digital mentoring and peer-to-peer support platforms complement school-based intervention.

IV.3. Technological solutions

Machine learning algorithms can detect aggressive language and abusive content, triggering automatic alerts or proactive moderation. However, their performance depends on linguistic and cultural context, and requires combination with human moderation and decision-challenge mechanisms (*Mahmud, Khan & Choudhury, 2023*). Platforms can implement “design frictions” (empathetic nudges, confirmation windows) to reduce the impulsiveness of hostile behaviors (*Metzler & Garcia, 2024, pp. 735–748*).

IV.4. Institutional role and public policies

Educational authorities, police and non-governmental organisations should work with digital platforms to establish clear reporting and intervention protocols. At the European level, the Digital Services Act (2024) imposes strong obligations on platforms to mitigate risks to user safety, and Member States must develop national support mechanisms for victims, including free psychological counselling and 24/7 helplines (*Husovec, 2024, pp. 70-72*).

V. LEGAL RESPONSE AND LEGISLATIVE CHALLENGES

V.1. Gaps in the national legal framework

In Romania, the phenomenon of cyberbullying does not currently benefit from an express and autonomous regulation in the Criminal Code. The term ”cyberbullying” is missing from the normative corpus, which creates difficulties in legal qualification and, implicitly, in protecting victims and sanctioning perpetrators. Associated behaviors are usually classified as already existing crimes, such as:

- harassment (art. 208 Criminal Code);
- threat (art. 206);
- psychological violence - bullying (introduced in the National Education Law by Law no. 221/2019);
- violation of privacy (art. 226);
- child pornography (art. 374);
- violation of the secrecy of correspondence (art. 302);
- computer forgery (art. 325) or illegal access to an information system (art. 360).

Of these, the closest to digital harassment is the regulation in art. 208 paragraph (2) of the Criminal Code, which defines an aggravated form of harassment that includes: “making telephone calls or sending communications by any means of remote transmission, which, by frequency or content, causes the victim a state of fear” (Criminal Code, 2009, updated) [1].

This provision, however, has important limitations: it does not fully cover the multiple dimensions of digital aggression, such as sharing images, impersonation, trolling or using social platforms for defamation. At the same time, it requires proof of a state of fear, a condition that is difficult to objectify and prove in court (*Cioclei, 2024, p. 156*).

V.2. ECHR case law

In recent years, the European Court of Human Rights (ECHR) has provided an increasingly broad interpretation of Articles 3 and 8 of the Convention, recognizing the serious impact of cyberbullying on individuals’ fundamental rights, particularly in contexts of gender-based violence, privacy and degrading treatment. Although there is still no case that directly addresses

[1] Law no. 286 of 2009, published in the Official Journal of Romania no. 510 of 24 July 2009.

"cyberbullying" in the established sense of the term, several relevant judgments have addressed concrete forms of cyberbullying, contributing to the consolidation of a jurisprudence in the field.

a) Buturugă v. Romania (11 February 2020)

A landmark in European jurisprudence on the recognition of cyberbullying as a form of violence is the ECHR Judgment in the case of Buturugă v. Romania. The applicant accused the Romanian authorities of failing to effectively investigate allegations of illegal access by her ex-partner to her email and Facebook accounts, as well as the misuse of personal data, thus claiming that she was the victim of a series of acts of domestic and digital violence (unauthorised access to her accounts, copying and use of personal messages and images).

Curtea Europeană a Drepturilor Omului a constatat încălcarea art. 3 (interzicerea tratamentelor inumane sau degradante) și a art. 8 (dreptul la viață privată) din Convenția Europeană a Drepturilor Omului, reținând că statul român nu și-a îndeplinit obligația pozitivă de a proteja viața privată a reclamantei și de a investiga eficient faptele reclamate (*CEDO, 2020*).

The ECHR has expressly stressed that: "digital intrusions into private life, such as telephone surveillance or illegal access to personal accounts, represent modern forms of domestic violence that must be treated with the same seriousness as physical abuse" (*Buturugă v. Romania, §76–80*).

This decision practically enshrines the recognition of cyberviolence as a dimension of gender-based violence and requires member states to adapt their legislation and protection mechanisms.

b) Volodina v. Russia (September 14, 2021)

An important precedent set after the Buturugă v. Romania case is the decision of the European Court of Human Rights in the Volodina v. Russia case, which aims to extend the recognition of digital abuse as degrading treatment.

In this case, the applicant was the victim of repeated acts of digital surveillance, intimidation through messages, tracking with GPS devices, unauthorized access to online accounts and storage of private materials.

The Court found a violation of Article 3 of the Convention, considering that this type of digital surveillance and control constitutes a form of degrading treatment, with psychological effects comparable to physical violence. The Court held that the Russian authorities failed to adopt effective measures to prevent and sanction these acts, thus violating the positive obligations imposed by Article 3 of the Convention (prohibition of inhuman and degrading treatment). The Russian state was sanctioned for failing to ensure an effective legislative and institutional framework for protecting the victim and investigating the facts (*ECHR, 2021*).

The ECHR has stressed that: "States have a positive obligation to protect vulnerable persons against modern forms of abuse, including those facilitated by electronic or digital means" (*Volodina v. Russia (No. 2), §90–93*).

It has thus highlighted the intersection between technology and domestic violence, recognising that cyberviolence in intimate relationships must be treated with the same seriousness as traditional forms of aggression. The Court has also reiterated the importance of effectively investigating such complaints and providing victims with a real remedy.

c) M.Ș.D. v. Romania (December 3, 2024)

A more recent and particularly relevant case for cyberbullying is M.Ș.D. v. Romania, in that it explicitly recognises cyberbullying as a form of gender-based violence, extends the State's obligations to adapt criminal law to new digital risks and requires the authorities to exercise rigorous procedural diligence in investigating digital crimes, including in the absence of direct physical violence.

In this case, the Court examined a complaint lodged by a young woman who had been subjected to a campaign of cyberbullying through identity theft, the publication of defamatory content and the distribution of personal images without consent, all carried out by her former partner. The applicant argued that the national authorities had downplayed the seriousness of the acts and had failed to conduct an effective investigation.

The Court held that there had been a violation of Art. 8 of the Convention, emphasizing that:"When the State fails to protect individuals – especially women – from emerging forms of violence facilitated by technology, the right to private life and personal security is violated." (*M.Ș.D. v. Romania, §102*)

d) Relevance for national regulations

The ECHR judgments in the cases of Buturugă v. Romania (2020), Volodina v. Russia (2021) and M.Ș.D. v. Romania (2024) outline a robust jurisprudential framework for the recognition and sanctioning of digital violence. Buturugă enshrined the state's obligation to effectively investigate cyberbullying and illegal access to personal data, treating it as a form of gender-based violence protected by art. 3 and 8 ECHR. Volodina expanded the interpretation of these articles, emphasizing that digital bullying should not be analyzed in isolation, but in the context of abusive relationships, where cyber surveillance, manipulation of information and online threats can have effects comparable to physical violence. The M.Ș.D. argued for the first time that cyberharassment and digital identity theft constitute serious forms of violence against women and children, requiring the existence of a coherent legal framework and effective remedies. Together, these cases require states, including Romania, to distinctly criminalize serious forms of cyberviolence, adapt criminal procedures to technological realities and ensure rapid and effective protection for victims, aligning national legislation with ECHR standards and European initiatives such as the Digital Services Act.

V.3. Current legislative challenges

The absence of an autonomous criminalization of cyberbullying in Romanian criminal law generates multiple practical and conceptual difficulties. First, the existing legal instruments do not reflect the technological specificity of

these acts, which leads to incomplete or forced classifications. Second, the administration of evidence is often hampered by online anonymity and the cross-border nature of digital communication. In addition, there is no coherent system of victim protection, especially in the case of minors, and judicial practice is uneven, with divergent solutions for similar acts. Romania has also not yet implemented a legislative mechanism dedicated to combating digital bullying in the school environment, although Law 221/2019 amending and supplementing National Education Law No. 1/2011 - on psychological violence/bullying, also includes digital forms of bullying in its definition[2].

Implications for Romanian law and European standards. Recent ECHR jurisprudence – in particular the Buturugă, Volodina and M.Ș.D. cases – confirms the need to recognise and sanction digital harassment as a form of violation of fundamental rights. From a national perspective, these standards require:

- revising the Criminal Code to explicitly introduce the crime of cyber harassment;
- expanding the procedural framework for the efficient investigation of acts committed by electronic means;
- strengthening the protection of victims, especially in cases of gender-based violence, where technology is used as a means of control and intimidation.

At the same time, Romanian legislation needs to be aligned with European trends, such as the Digital Services Act (2024), which imposes concrete obligations on online platforms to moderate abusive content, and recent initiatives of the European Commission on combating online violence against women and girls.

V.4. European law and harmonisation trends

At the European Union level, despite the existence of regulations on cybercrime (e.g. the Budapest Convention, Directive 2011/92/EU on combating child sexual abuse[3], or the GDPR Regulation), there is no uniform criminalization of cyberbullying as a distinct crime.

The EU's recently adopted Directive (EU) 2024/1385 on combating violence against women and domestic violence[4] criminalises at EU level several forms of *cyberviolence* under Article 83 TFEU. These include the non-consensual sharing of intimate or manipulated material (such as deepfakes), cyberstalking, cyber harassment, and the non-consensual recording of intimate material. The Directive goes beyond earlier calls of the European

[2] Law no 221/2019 published in the Official Journal of Romania no. 929 of 19 November 2019.

[3] Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse, sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, (published in *OJ L 335, 17.12.2011, pp. 1–14I)*

[4] Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence, (published in *OJ L 2024/1385, 24.5.2024)*

Parliament's 2022 resolution on cyberbullying against women and girls[5], which urged the Commission to issue a binding legal act to prohibit the distribution of sexualised content without consent, to criminalise practices such as doxxing and online hate speech, and to introduce rapid mechanisms for the removal of harmful online content.

Also, the Digital Services Act (DSA) Legal Framework, which came into force in 2024, imposes strict obligations on digital platforms to moderate illegal content, including harassment and hate speech, providing a new protection tool for users.

In conclusion, the absence of a clear regulation of cyberbullying in the Romanian Criminal Code and the lack of harmonisation at EU level creates a vacuum of normative protection. It is necessary to develop a coherent criminal policy, based on contemporary social and technological realities, supported by ECHR jurisprudence and international human rights standards.

VI. RECOMMENDATIONS AND PUBLIC POLICIES

Effectively combating cyberbullying requires a multidimensional approach, combining legislative, technological, educational and institutional instruments. The analysis presented above clearly indicates the existence of significant gaps in the Romanian legal framework, the insufficiency of preventive resources and the lack of integrated public policies. Therefore, a set of concrete and coherent measures is needed, subsumed under a broader objective: ensuring a safe, inclusive and responsible digital environment.

VI.1. Legislative measures

In order to ensure effective protection against cyberbullying and align it with European and international standards, the following legislative directions must be adopted:

1). Autonomous criminalization of cyberbullying in the Criminal Code, by introducing a distinct offense that captures the specifics of this phenomenon – the anonymity of the perpetrators, the speed and extent of dissemination, identity theft and the use of electronic means for abusive purposes.

2). Revision of Art. 208 of the Criminal Code (harassment) to expressly include forms of cyberviolence as an aggravating circumstance, in accordance with the ECHR jurisprudence in the Buturugă, M.Ș.D. and Volodina cases.

3). Establishment of a specific regulatory framework for the protection of minors in the digital environment, which would provide for sanctions applicable to companies that tolerate or do not promptly remove abusive content from their platforms.

[5] European Parliament. (2022). European Parliament resolution of 5 July 2022 on cyberviolence and cyberbullying against women and girls (2021/2035(INI)).

4). Harmonization of national legislation with recent European legal instruments, including:

- Digital Services Act (Regulation (EU) 2022/2065)[6], which establishes clear responsibilities for online platforms in moderating illegal and harmful content;

- Directive on violence against women and domestic violence (Directive (EU) 2024/1385)[7];

- Istanbul Convention [8] , which imposes strong legislative and administrative measures to combat gender-based violence, including in the digital environment.

Combating cyberbullying requires a preventive and formative approach, by integrating the digital dimension into educational and social policies:

- Introducing digital education into the national curriculum at all levels of education, with modules dedicated to online security, digital rights and responsibilities, informed consent in the digital environment and recognition of abusive behaviors in networks;

- Implementing prevention programs in schools, carried out through partnerships between the Ministry of Education, local authorities, non-governmental organizations and school psychologists, which should include interactive workshops and practical simulations;

- Conducting national awareness campaigns on the risks and consequences of cyberbullying, addressed to adolescents, parents and teachers, using visual communication channels adapted to the target audience (social media platforms such as TikTok, YouTube, Instagram);

- Continuous professional training of teachers and staff from public order structures, for the early identification and appropriate management of cyberbullying cases, including by familiarizing them with rapid reporting tools and effective intervention procedures.

VI.2. Technological and administrative measures

Preventing and combating cyberbullying cannot be achieved exclusively through legislative or technological changes. A paradigm shift is needed in education, in digital culture and in the way society responds to new forms of violence. Only through an integrated national strategy, supported by inter-

[6] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), (published in *OJ L 277, 27.10.2022, pp. 1–102).*

[7] Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence, (published in *OJ L, 2024/1385, 24.5.2024*)

[8] Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence (the Istanbul Convention) ratified by Romania through Law no. 30/2016 on May 23, 2016.

institutional cooperation and dialogue with private actors, can a safer, more inclusive and more responsible online environment be built for all citizens, especially for young people and vulnerable groups.

Thus, reducing the impact of cyberbullying also requires the implementation of efficient technological tools and administrative mechanisms, with the involvement of both public authorities and private actors:

- Legal obligations for online platforms to implement automatic filters, intuitive reporting systems and clear and restrictive terms of use regarding offensive content and abusive behavior;
- Public-private partnerships (Google, Meta, TikTok, etc.) to develop solutions based on artificial intelligence, capable of detecting and limiting the spread of potentially abusive content before it goes viral;
- Establishment of a national digital registry of complaints regarding online harassment, interconnected with the police, courts and the main social platforms, in compliance with personal data protection standards under the supervision of the National Authority for the Supervision of Personal Data Processing;
- Free psychological support services for victims, including emergency hotlines and anonymous online chats, operated by specialists in counseling and crisis intervention.

CONCLUSION

Cyberbullying is one of the most current and dangerous manifestations of violence in the digital age. The diversity of forms of aggression, the difficulty of identifying perpetrators and the profound psychological impact on victims transform this phenomenon into a major challenge for legal systems, educational institutions and society as a whole.

This paper has analyzed cyberbullying from an interdisciplinary perspective, approaching it both as a social and psychological phenomenon and as a legal issue. The defining characteristics of cyberbullying — the intention to harm, the repetitive nature, the imbalance of power and the anonymity of the aggressor — as well as the behavioral typologies associated with it have been highlighted. Gender and age differences, as well as the emotional and social effects of digital victimization have also been explored.

The analysis of the national legal framework revealed the absence of a clear and autonomous criminalization of cyberbullying in the Romanian Criminal Code, which creates a vacuum of normative protection. In this regard, the recent case law of the European Court of Human Rights — in particular the cases of Buturugă v. Romania (2020), Volodina v. Russia (No. 2) (2021) and M.Ş.D. v. Romania (2024) — provides important guidelines on the interpretation of Articles 3 and 8 of the Convention in the context of digital abuse, reinforcing the positive obligation of states to protect citizens from technologically facilitated violence.

The paper finally proposes a series of legislative, educational and institutional recommendations aimed at underpinning a coherent public policy to prevent and combat cyberbullying. Not only an update of criminal norms is needed, but also a change of approach, involving school, family, digital platforms and authorities in a joint effort to guarantee online safety. Combating cyberbullying is not just a matter of legislation, but one of social culture and collective responsibility.

BIBLIOGRAFIE

1. Cioclei, V. (2024). Drept penal. Partea specială. Vol. II. Infracțiuni contra persoanei. Bucharest: C.H. Beck Publishing House.
2. Citron, D. K. (2014). *Hate crimes in cyberspace*. Harvard University Press.
3. Estévez, E., Cañas, E., Estévez, J. F., & Povedano, A. (2020). Continuity and overlap of roles in victims and aggressors of bullying and cyberbullying in adolescence: A systematic review. *International Journal of Environmental Research and Public Health, 17*(20),7452. https://doi.org/10.3390/ijerph17207452
4. European Court of Human Rights. (2020, 11 february). Case of *Buturugă v. România*. https://hudoc.echr.coe.int/fre?i=001-201342
5. European Court of Human Rights. (2021, 14 september). Case of *Volodina v. Russia (No. 2)*. https://hudoc.echr.coe.int/fre?i=001-211794
6. European Court of Human Rights. (2025, april). Case of *M.Ș.D. v. România*. Strasbourg Observers. https://strasbourgobservers.com/2025/04/22/strasbourgs-consolidation-on-technology-facilitated-gender-based-violence-m-s-d-v-romania/
7. Hay, C., Meldrum, R. C., & Mann, M. (2010). Bullying victimization and adolescent self-harm. *Youth Violence and Juvenile Justice, 4*(2), 148–169. https://doi.org/10.1007/s10964-009-9502-0
8. Hellfeldt, K., López, A. B., & Andershed, H. (2020). Cyberbullying and psychological well-being in young adolescents: The potential mediational role of perceived social support from family friends and teachers. *International Journal of Environmental Research and Public Health, 17*(1), 45. https://doi.org/10.3390/ijerph17010045
9. Huang, J., Zhong, Z., Zhang, H., & Li, L. (2021). Cyberbullying in social media and online games among Chinese college students and its associated factors. *International Journal of Environmental Research and Public Health, 18*(9), 4819. https://doi.org/10.3390/ijerph18094819
10. Husovec, M. (2024). The Digital Services Act's red line: What the Commission should not do to very large online platforms. *Journal of Cyber Policy, 9*(2), 254–274. Husovec, Martin, The Digital Service Act's Red Line: What the Commission Can and Cannot Do About Disinformation (January 10, 2024). Available at SSRN: https://ssrn.com/abstract=4689926. or http://dx.doi.org/10.2139/ssrn.4689926

11. Kasturiratna, K. T. A. S., Hartanto, A., Chen, C. H. Y., Tong, E. M. W. & Majeed, N. M. (2024). Umbrella review of meta analyses on the risk factors, protective factors, consequences and interventions of cyberbullying victimization. *Nature Human Behaviour*. https://doi.org/10.1038/s41562-024-02011-6
12. Kowalski, R. M., Giumetti, G. W., Schroeder, A. N., & Lattanner, M. R. (2014). Bullying in the digital age: A critical review and meta-analysis of cyberbullying research among youth. *Psychological Bulletin, 140*(4), 1073–1137. https://doi.org/10.1037/a0035618
13. Livingstone, S., & Görzig, A. (2014). When adolescents receive sexual messages on the internet: Explaining experiences of risk and harm. *Computers in Human Behavior, 33*, 8–15. https://doi.org/10.1016/j.chb.2013.12.021
14. Mahmud, T., Khan, M. U., & Choudhury, S. M. (2023). Cyberbullying detection for low-resource languages and dialects: Review of the state of the art. *Information Processing & Management, 60*(5), 103454. https://doi.org/10.1016/j.ipm.2023.103454
15. Metzler, H., & Garcia, D. (2024). Social drivers and algorithmic mechanisms on digital media: Implications for online harm reduction. *Perspectives on Psychological Science, 19*(5), 735–748. https://doi.org/10.1177/17456916231185057
16. Menesini, E., & Salmivalli, C. (2017). Bullying in schools: The state of knowledge and effective interventions. *Psychology, Health & Medicine, 22*(1), 240–253. https://doi.org/10.1080/13548506.2017.1279740
17. Monteiro, A. P., Marques, F., Relva, I. C., Simões, M., Sani, A. I., & Correia, E. (2024). The Relation Between Bullying and Cyberbullying, Emotional Intelligence, and Empathy in Portuguese Adolescents. *Adolescents*, *4*(4), 620-634. https://doi.org/10.3390/adolescents4040043
18. Montero-Fernández, D., López-Sebastián, A., & Del Moral-Pascual, M. (2023). *Click Surveillance of Your Partner! Digital Violence among Young Couples. Social Sciences, 12*(4), article 203. https://www.mdpi.com/2076-0760/12/4/203
19. Olweus, D. (1999). *Bullying at school: What we know and what we can do*. Oxford: Blackwell Publishing.
20. Patchin, J. W., & Hinduja, S. (2006). Bullies move beyond the schoolyard: A preliminary look at cyberbullying. *Youth Violence and Juvenile Justice, 4*(2), 148–169. https://doi.org/10.1177/1541204006286288
21. Polanin, J. R., Espelage, D. L., Grotpeter, J. K., Ingram, K., Michaelson, L., Spinney, E., Valido, A., & Robinson, L. E. (2022). A systematic review and meta-analysis of interventions to decrease cyberbullying perpetration and victimization. *Prevention Science, 23*(3), 439–454. https://doi.org/10.1007/s11121-021-01259-y
22. Pornari, C. D., & Wood, J. (2010). Peer and cyber aggression in secondary school students: The role of moral disengagement, hostile attribution bias, and

outcome expectancies. *Aggressive Behavior, 36*(2), 81–94. https://doi.org/10.1002/ab.20336
23. Ray, G., McDermott, C. D., & Nicho, M. (2024). Cyberbullying on social media: Definitions, prevalence, and impact challenges. *Journal of Cybersecurity, 10*(1), tyae026. https://doi.org/10.1093/cybsec/tyae026
24. Ševčíková, A., & Šmahel, D. (2009). Online harassment and cyberbullying in the Czech Republic: Comparison across age groups. *Zeitschrift für Psychologie / Journal of Psychology, 217*(4), 227–229. https://doi.org/10.1027/0044-3409.217.4.227
25. Sorrentino, A., Sulla, F., Santamato, M., di Furia, M., Toto, G. A., & Monacis, L. (2023). Has the COVID-19 pandemic affected cyberbullying and cybervictimization prevalence among children and adolescents? A systematic review. *International Journal of Environmental Research and Public Health, 20*(10), 5825. https://doi.org/10.3390/ijerph20105825
26. Slonje, R., & Smith, P. K. (2008). Cyberbullying: Another main type of bullying? *Scandinavian Journal of Psychology, 49*(2), 147–154. https://doi.org/10.1111/j.1467-9450.2007.00611.x
27. Slonje, R., Smith, P. K., & Frisén, A. (2012). The nature of cyberbullying, and strategies for prevention. *Computers in Human Behavior, 29*(1), 26–32. https://doi.org/10.1016/j.chb.2012.05.024
28. Smith, P. K. (2012). Cyberbullying and its impact on young people's emotional health and well-being. In P. K. Smith & G. Steffgen (Eds.), *Cyberbullying through the new media: Findings from an international network* (pp. 27–40). Psychology Press.
29. Thacker, S., & Griffiths, M. D. (2012). *An exploratory study of trolling in online video gaming. International Journal of Cyber Behavior, Psychology and Learning, 2*(4), 17–33. https://doi.org/10.4018/ijcbpl.2012100102
Weekes, C.J., Storey, J.E. & Pina, A. (2025). Cyberstalking Perpetrators and Their Methods: A Systematic Literature Review. *Trauma, Violence & Abuse*. Sage Publications. 2025 Apr 24. https://doi.org/10.1177/15248380251333411.