

Cyberbullying and Online Harassment: Gaps in Current Legal Protections

Jyoti Verma¹ and Dr. Jyoti Yadav²

Criminal Law¹

Assistant Professor²

Amity University Lucknow, Uttar Pradesh, India

Abstract: *Cyber harassment and cyberbullying are common problems in the information age that cut across all age groups globally. With growing dependency on internet-based communication tools, these issues have resulted in great psychological and emotional trauma to victims. Though there is heightened awareness, existing legislation frequently lacks adequate protection or is unable to deter perpetrators. This paper discusses the current legal safeguards against cyberbullying and online harassment and identifies major gaps in the law that make effective enforcement and victim assistance difficult. These gaps involve conflicting definitions of cyberbullying, jurisdictional issues, and lack of responsibility for online platforms. The paper also discusses the incapacities of laws like Section 230 of the Communications Decency Act and the international nature of internet-based crimes that hinder legal processes. Accordingly, this paper investigates some solutions like international legal collaboration, revisions to Section 230, and better systems of supporting victims. Furthermore, the researchers stress the requirement of technological innovations and information campaigns, as well as education campaigns to foster secure online cultures. Ultimately, the paper advocates for stronger legal frameworks that adapt to the evolving nature of online interactions, ensuring greater protection for victims and greater accountability for offenders.*

Keywords: Cyberbullying, Online Harassment, Legal Protections, Digital Communication, Victim Support

I. INTRODUCTION

The rapid expansion of digital communication platforms and social media over the past two decades has fundamentally transformed the way individuals interact with one another. Although these technologies have ushered in many advantages, such as simpler communication, increased global connectivity, and the democratization of information, they have also brought about serious risks. Among them, cyberbullying and online harassment have become widespread problems that impact millions of people globally. These acts, which take place in online communities like social media sites, messaging applications, and online gaming groups, have resulted in extreme emotional, psychological, and even physical damage for the affected victims.

The frequency of cyberbullying and online harassment is high. The Pew Research Center¹ estimates that almost 59% of U.S. teenagers report some sort of cyberbullying, with most victims suffering from serious emotional distress as a consequence. The anonymity facilitated by online platforms enables perpetrators to commit abusive actions with minimal risk of identification or legal repercussions, which aggravates the situation. Victims themselves usually experience difficulties in pursuing justice, as they might lack the expertise in gathering digital evidence, jurisdictional restrictions, and minimal assistance from current legal frameworks.

With the ongoing evolution of the digital world, strong legal safeguards against cyberbullying and online harassment have become increasingly imperative. Yet, in spite of numerous national and international initiatives, present legal frameworks fall short in dealing with the intricacies brought by the internet. These shortcomings are a result of problems regarding inconsistent definitions of cyberbullying, difficulties in enforcing law across international boundaries, and the absence of responsibility for online platforms hosting offensive content.

¹Pew Research Center. (2018). "The State of Online Harassment." Retrieved from <https://www.pewresearch.org>



This essay examines these loopholes in legal safeguards and critically assesses the efficacy of current legislation in addressing cyberbullying and online harassment. Through a critical examination of both the strengths and weaknesses of current legal strategies, this essay seeks to shed light on how the law can be improved to more effectively counter the challenges of these emerging problems. From this examination, the paper aims to suggest responses that can strengthen legal protection for victims, heighten accountability for offenders, and secure better online environments for everyone.

Section 1: Definition and Scope of Cyberbullying and Online Harassment

The digital age has brought forth a variety of new challenges, and perhaps the most acute are those of cyberbullying and online harassment. These two terms are frequently applied interchangeably, but they designate different forms of negative conduct that take place online. Getting a grasp on the subtleties of this behavior is key to developing the proper legal responses and protections.

Cyberbullying is a deliberate utilization of online platforms, including social media, text messages, or websites, to hurt, intimidate, or manipulate another person. Cyberbullying is usually through repeated efforts to exert dominance or control over a victim. The types of cyberbullying are varied and can range from verbal abuse (such as name-calling or insults), social exclusion (such as deliberately excluding someone from online group activities or discussions), spreading false rumors or lies, and doxxing—the public disclosure of private or sensitive information about a person without their permission. The defining characteristic of cyberbullying is its repetition and its use of technology to pursue the victim, which makes it especially pernicious and hard to avoid since electronic communications can track the victim down anywhere and at any time.

Online harassment, although frequently coinciding with cyberbullying, is a more general category of abusive behaviors. These are stalking (ongoing and unwanted pursuit, typically with an aim to intimidate), threats of violence, defamatory communications, impersonation, and other types of psychological abuse. Harassment can be directed toward a single person, a group, or a whole community and can take place via one or more of a range of online mediums, such as social media, email, chat rooms, and online forums. In contrast to cyberbullying, which is often committed by peers or people with some form of social or personal association with the victim, online harassment may be perpetrated by total strangers, rendering victims' anticipation of, and preparation against, it even more improbable.

The prevalence of both cyberbullying and online harassment has resulted in an international outcry and an explosion of both national and international initiatives to create legal frameworks to combat these phenomena. Nations like the United States, the United Kingdom, Australia, and India have passed specific legislation intended to combat different types of online harm. Globally, efforts such as the European Union's General Data Protection Regulation (GDPR)² and initiatives by the United Nations strive to present guidelines for the protection of users online. Despite these efforts, the success of legal actions has been hampered by a number of challenges.

One of the biggest challenges is the absence of clear and consistent definitions of what constitutes cyberbullying and online harassment. Various jurisdictions employ different terminologies and criteria, and that makes it difficult to establish universal legislation or agreements. In other jurisdictions, behaviors that could be classified as online harassment or bullying may not be classed as criminal offenses in current legal frameworks.

A major problem is the jurisdictional complexity presented by the global nature of the internet. Cyberbullies and online harassers can often act from beyond national borders, rendering it impossible for national legislation to offer definite protection or hold them to account. Anonymity created by the internet also makes it harder, and in some cases impossible, to conceal identities behind IP addresses and evade detection or prosecution.

Third, there is the problem of translating old legal rules into an electronic space. Harassment or bullying statutes that are created with the intention of addressing these activities in brick-and-mortar settings are not well-suited to deal with the subtleties of cyberconduct, where anonymity, rapidness, and an expansiveness of impact are the norm. The electronic space introduces novel manners of causing harm and many of the current laws neglect to effectively embrace these novel methods of abuse.

²European Parliament. (2016). "General Data Protection Regulation (GDPR)." Official Journal of the European Union. Retrieved from <https://gdpr.eu>



In conclusion, though both online harassment and cyberbullying are detrimental and ubiquitous, the legal environment has difficulty keeping up with the fast pace of the evolution of digital communication technologies. The loopholes in definitions, jurisdiction, and applicability of prevailing legal frameworks illustrate the imperative for holistic reforms that more adequately respond to the intricacies of abuse online during the digital era.

Section 2: Current Legal Protections

In response to increasing concerns about cyberbullying and online harassment, a number of nations have established legal frameworks to address these issues. Although these efforts have afforded some measure of protection, numerous challenges continue to exist in implementing effective and overarching laws to deal with the intricacies of online behavior. This section will review the current legal protections in prominent nations, such as the United States, the European Union, India, and Australia, and point out the shortcomings of these frameworks.

United States

There have been several laws enacted in the United States to address cyberbullying and online harassment. Among the most significant laws enacted is the Megan Meier Cyberbullying Prevention Act, which aims to criminalize certain online activities that cause injury, such as cyberbullying and harassment. The aim of the act is to make the perpetrators liable by declaring online bullying as an offense that can be punished, especially if the bullying causes severe emotional distress. But though the law has drawn attention, it is yet to be enacted into law at the federal level.

Another of the key legislations is the Communications Decency Act (CDA) of 1996, specifically Section 230. Under this provision, internet platforms, including social media websites, are given immunity from liability for user postings. Whereas Section 230 has helped the internet flourish by giving protections to platforms to not face liability, it has been much disapproved for enabling platforms to shun accountability where it pertains to cyberbullying³ and harassment. Such an immunity makes the platforms sidestep responsibility when users' uploaded harmful content leads to such action. The actions lead to slowing or lack of responses where removal of abusive posts are involved. Critics hold the argument that this legal protection needs to be reviewed or reformed, particularly in relation to cyberbullying and harassment on the internet.

European Union

In the European Union, the General Data Protection Regulation (GDPR) has provided some degree of protection for people in the online arena, especially via the "right to be forgotten." The GDPR gives people the right to have their personal details erased from websites, which can be especially beneficial for victims of online abuse who want to retake control over their personal data. In addition, the regulation makes tough requirements on platforms to process personal data responsibly and protect the privacy of users.

Nevertheless, while the GDPR has put into place crucial privacy measures, it lacks effectiveness in regulating online harassment and cyberbullying. The law does not expressly criminalize the behavior of harassment or bullying, leaving much of the protection from the law lacking for victims. Additionally, the international character of the internet makes enforcement of these safeguards challenging, since websites are commonly based in foreign countries, rendering it hard to implement EU regulations across the board. Consequently, most instances of online harassment go unpunished.

India

In India, online harassment is addressed by the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (2011), which place obligations upon platforms to keep sensitive personal data secure and protect users in general from online harms. The legislation grants some degree of protection from cyberbullying in that the platforms have to take reasonable measures to counter improper use of personal data and

³Livingston, J. (2019). "International Cyberbullying Laws: A Comparative Analysis." *Journal of Internet Law*, 22(6), 23-47.



also act promptly in response to harassment. Yet, its enforcement has been sporadic, and its laws contain no clear definitions of cyberbullying or online harassment.

Furthermore, there is no complete legal code that is specifically tailored towards the entire range of cyberbullying and online harassment within India. The available legal safeguards are mainly concerned with data security and privacy instead of psychological damage resulting from online bullying. This is due to the fact that the gap in legal definitions and enforcement difficulties has yielded limited success in addressing cyberbullying in India.

Australia

Australia has made efforts to tackle cyberbullying through the Enhancing Online Safety Act 2015, which established the Office of the eSafety Commissioner. The office is responsible for examining complaints of online harassment and cyberbullying, especially for children and young adults. The Act empowers the Commissioner to examine complaints and issue removal notices to online service providers who host offending content. Furthermore, the bill permits people to report cases of online harassment directly to the Commissioner, giving a direct route for victims to gain assistance.

While the Enhancing Online Safety Act is a step in the right direction, there are issues with its enforcement. As in other nations, Australia is also confronted by jurisdictional concerns since most of the sites targeted for cyberbullying are operated abroad, making it difficult to enforce domestic law. Further, the law concentrates mostly on children and lacks adequate protection for adults, creating a lacuna in the law to cover protection at large.

Limitations of Existing Legal Frameworks

Notwithstanding the initiatives undertaken by different countries, there are some limitations to the legal frameworks put in place to address cyberbullying and online harassment:

1. Lack of Clear Definitions

Most existing legislation does not have clear and consistent definitions of what constitutes cyberbullying and online harassment. This creates difficulties in applying legal standards across different jurisdictions and in effective enforcement.

2. Jurisdictional Challenges

The global nature of the internet means that online harassment and cyberbullying often involve individuals or platforms located in different countries. This creates significant jurisdictional issues, as laws designed to address these issues are often limited by national borders. International cooperation is often lacking, which further complicates the enforcement of protections for victims.

3. Limited Enforcement Mechanisms

In most instances, the laws are on the books but not practically enforced. The absence of capability, training, and expertise among law enforcement to manage cybercrimes, and the anonymity provided by the internet, renders it hard to punish culprits.

4. Platform Immunity

In other jurisdictions, for example, the United States, legislation like Section 230 of the Communications Decency Act shields platforms from liability for the content created by users. This protection from the law denies victims the right to hold platforms liable for the harmful content they provide, posing a major barrier to combating cyberbullying and harassment.

In summary, while there have been advances in various nations addressing cyberbullying and online harassment through law, there are still significant gaps in these protections. Specifically, problems concerning the definition of online harm, jurisdictional issues, and platform accountability must be resolved in an effort to develop better legal responses to these endemic problems.

Section 3: Gaps in Current Legal Protections

Even with efforts from different nations to respond to cyberbullying and online intimidation, there exist quite a number of vulnerabilities in the existing legal protection available to victims. The gaps work to dilute the effectiveness of the



available laws and enable the criminals to go scot-free. Below are some of the most important issues that affect the capability of the available legal frameworks to offer adequate protection.

1. Lack of Clear Definitions and Standards

One of the biggest difficulties in combating cyberbullying and online harassment is the absence of consistent and straightforward definitions of such behaviors throughout jurisdictions. The term "harassment," for instance, has varying meanings within countries, regions, or systems of law. Some legislation is concerned with threats of violence or stalking, whereas others include wider forms of psychological or emotional abuse. This disparity renders it challenging to have a standard legal criterion universally accepted and, more often than not, causes discrepancies in the treatment of cases.

For example, "cyberbullying" in America might not necessarily match how it is legally defined in the European Union or India. In some nations, purely online bullying may not qualify as harassment unless combined with other direct harm. Such inconsistencies not only cause confusion but also hinder the uniform enforcement of laws. The lack of clear and universally applicable definitions is a factor in the challenge of developing cohesive and effective legal protections that can be enforced everywhere.

2. Jurisdictional Issues

The international nature of the internet makes it difficult to enforce national laws against cyberbullying and online harassment. The internet knows no geographical boundaries, and perpetrators can target victims across countries, making it difficult to enforce national laws. A perpetrator might be in one country, the victim in another, and the platforms hosting the offensive content in a third country altogether.

These jurisdictional matters complicate it for law enforcement agencies to track and prosecute offenders. For instance, an individual in one nation can harass another person in a different nation through social media or email, and national laws will not have the jurisdiction or the enforcement capabilities to deal with the conduct. In addition, global cooperation rarely exists, and countries frequently don't have bi-lateral compacts that will provide for extraditing criminals or the enforcement of overseas laws. That lack of coordination in the global legal establishment renders many victims powerless and facilitates criminals' conducting affairs with minimal restraint.

3. Section 230 of the Communications Decency Act

In the United States⁴, Section 230 of the Communications Decency Act has been a central issue in the controversy surrounding online harassment and cyberbullying. Section 230 grants wide immunity to online platforms, shielding them from liability for user content. Although this provision was initially intended to promote the development of the internet by keeping platforms from being responsible for all material posted by users, it has been widely denounced for allowing platforms to escape liability for abusive material, such as cyberbullying and harassment.

The legal immunity afforded by Section 230 has hindered the ability of victims of online harassment to hold platforms liable. Platforms do not always react swiftly or effectively to eliminate abusive content, and even if they do, the damage is already done. Section 230 has been faulted for enabling platforms to avoid liability for failing to proactively stop cyberbullying or for failing to step in when abusive content is reported. The absence of liability promotes a culture of doing nothing and undermines initiatives to safeguard users against harassment and bullying. Several advocates have urged changes to Section 230 to hold platforms more accountable for the content they carry.

4. Challenges of Enforcement

Even when there are legal protections, enforcement is a serious challenge. Much cyberbullying and online harassment goes unreported because victims feel helpless, humiliated, or fear retaliation. Even if cases are reported, victims find it very difficult to navigate the justice system. This is especially the case for victims who might lack access to legal resources or support, which hinders them from seeking justice.

⁴United States Congress. (1996). "Communications Decency Act, Section 230." Retrieved from <https://www.congress.gov>



Law enforcement authorities also have significant challenges in addressing cybercrimes since most officers lack proper training to deal with cases of digital evidence or online conduct. Moreover, the internet's anonymity makes it hard to trace culprits, thus complicating the investigation process further. Most law enforcement agencies do not have the technical skills and resources to investigate sophisticated cybercrimes, resulting in delays or inability to prosecute offenders. Consequently, victims will feel that their cases do not matter, and the justice system is unable to offer them the protection they require.

5. Protection of Anonymity

The anonymity provided by the internet is double-edged. As it can safeguard people's privacy and freedom of expression, it also gives people a false sense of security, encouraging cyberbullies and harassers, as they feel comfortable carrying out harmful acts without the fear of exposure. This anonymity greatly complicates identifying the culprits, collecting evidence, and prosecuting them under current legal structures.

Some sites have brought in methods for confirming users' identities, but these remain insufficient, and agreement on how to balance the safeguarding of privacy against the imperative of making possible accountability for hurtful behavior on the net remains slight. Laws and regulatory arrangements covering net anonymity continue to lag behind, and few states have come forward to develop authoritative rules about how it should be addressed. The absence of regulations pertaining to anonymous web activity makes identification and prosecution difficult, leaving the victims exposed and unprotected.

Ultimately, although the law provides measures to counteract cyberbullying and online abuse, there exist glaring loopholes. These are mainly attributed to incoherent definitions, issues of jurisdiction, absence of accountability from platforms, enforcement constraints, and protection of anonymity. To be able to effectively fight cyberbullying and online harassment, these loopholes should be filled by legislative changes ensuring more precise definitions, increased responsibility of platforms, and better global collaboration. This is when a strong and efficient legal environment will be developed in order to safeguard victims and discourage abusers in the digital world.

Section 4: Proposed Solutions

To address the gaps in existing legal protection against cyberbullying and online harassment effectively, a number of solutions are needed to develop a more holistic and international response to these problems. The following recommendations seek to bolster legal frameworks, enhance enforcement, and offer more support to victims.

1. International Cooperation and Harmonization of Laws

One of the most important measures in addressing cyberbullying and online harassment is the establishment of international cooperation and harmonization of legislation. The international character of the internet means that online abuse tends to transcend borders, which can make enforcement and accountability more difficult. To counter this, nations must collaborate to establish standardized legal frameworks that define cyberbullying and online harassment uniformly and provide clear guidelines for enforcement. There can be international agreements or treaties set up to help cross-borders collaborate, such that the culprits who work from various bases can still be brought to justice.

For example, the Council of Europe's⁵ Convention on Cybercrime can be modified and used to sign a treaty containing specific provisions related to cyber harassment. This agreement would create a framework for international cooperation among nations, making extradition or enforcement of legal verdicts in instances of cyberbullying and online harassment easier.

2. Section 230 Reform

A crucial reform to prioritize in the United States is Section 230 reform of the Communications Decency Act (CDA). Although Section 230 has been essential in fueling internet development by immunizing platforms against liability for

⁵Council of Europe. (2001). "Convention on Cybercrime." Retrieved from <https://www.coe.int>



the content generated by their users, Section 230 has also enabled platforms to shun responsibility for harmful⁶ content hosted by them, including cases of harassment and cyberbullying.

Section 230 reform would make platforms more accountable for the content they host on their sites. Platforms should be obligated to take reasonable measures to avoid injurious content, such as proactively removing cyberbullying content and disciplining users who bully others. Platforms may also be obligated to offer assistance to victims by providing resources such as complaint avenues, counseling referrals, and educational material. This reform would balance the necessity for platform immunity with the duty to guarantee a respectful and secure online space.

3. Extension of Victim Support Services

Alongside the strengthening of legal protections, there also needs to be a prioritization of increasing victim support services. Legal frameworks are inadequate if victims of online harassment do not have the resources or the support necessary to access the legal system or manage the emotional and psychological impact of online harassment. Legal frameworks should be augmented by counseling, legal consultation, and online safety training.

Victims ought to be provided with extensive services that are suited to their requirements. Such services may be provided by public as well as private organizations and ought to be readily accessible, particularly in areas where legal safeguards are weak or poorly developed. Victim assistance programs may be incorporated into existing legal systems or provided by non-governmental organizations specializing in online safety. In certain instances, giving victims access to legal assistance can assist them in understanding complex legislation and gaining access to justice.

In addition, online safety training must be included in school education and community programs to inform people about the dangers of cyberbullying and online harassment, giving them the resources to defend themselves and obtain assistance if necessary.

4. Education and Awareness Campaigns

Another critical solution is the promotion of education and awareness campaigns. Governments, non-governmental organizations (NGOs), and advocacy groups should invest in initiatives to educate the public about the risks of cyberbullying and online harassment. These campaigns should aim to raise awareness about what constitutes online abuse, the psychological impact it can have on victims, and the steps individuals can take to protect themselves.

These campaigns can engage responsible digital citizenship by educating citizens on how to behave respectfully online, how to report abusive content, and how to assist others that are being harassed online. Educational programs can also make victims of cyberbullying less stigmatized, enabling more individuals to report cases of internet abuse.

Also, public education campaigns must address potential victims and offenders alike, teaching them about empathy, respect, and responsible use of online resources. Advertisements, social media campaigns, and outreach programs to reach out to people of different populations and online groups may be some of the efforts to be included.

5. Technological Solutions

Lastly, technological⁷ solutions are also important in preventing and reducing online harassment. Technology firms must invest in creating tools that can identify and block harassment in real time. The combination of machine learning (ML) and artificial intelligence (AI) may assist platforms in automatically marking content that is harmful, like abusive language or threatening behavior, before it is widely shared.

For instance, AI systems can be programmed to identify discriminatory or dangerous language, and machine learning programs might identify and mark patterns of online activity linked to harassment or cyberbullying. Sites also need to better equip users with reporting tools, so that it is simpler for people to report instances of harassment, and that these reports are reviewed quickly.

⁶Shaw, M. (2020). "The Limits of Section 230: Holding Platforms Accountable for Harmful Content." *Harvard Journal of Law and Technology*, 33(2), 255-274.

⁷Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, India. Ministry of Electronics and Information Technology, Government of India. Retrieved from <https://meity.gov.in>



In addition, sites might give users tools to shield themselves more actively, including content filters, privacy settings, and the option to block or mute harassing users. These technological advancements, in conjunction with good reporting and enforcement policies, could sharply decrease the occurrence of cyberbullying and online harassment.

Combating cyberbullying and online harassment needs to be addressed by a multi-pronged approach involving legal reform, victim assistance, educational efforts, and technological innovation. The solutions offered here seek to bridge the existing gaps in legal protections by enhancing international cooperation, updating platform liability laws, broadening victim support services, and investing in education and awareness-raising campaigns. Through an integrated approach to these efforts, governments, technology companies, and civil⁸ society organizations can collaborate to develop safer digital spaces where people can freely interact without fear of abuse or harassment.

II. CONCLUSION

Although efforts have been made to counter cyberbullying and online harassment, the legal protection that is available currently falls short in most cases. The fluid nature of communication online and the global jurisdiction of the internet demand a new and thorough legal structure that is capable of meeting this challenge. Current legislation is consistently found to be lacking on grounds such as variable definitions, territorial limitations, and lack of responsibility on the part of online mediums.

In order to strengthen legal safeguards, international cooperation is required to develop standardized frameworks that can be universally applied. Legislative changes, like those being suggested for Section 230 in the US, are necessary to make sure that platforms are held accountable for the content they host. Technological advancements such as AI-based content monitoring tools can also play a vital role in identifying and preventing abusive online behavior.

In addition, it is important to increase victim support services and awareness through education and public campaigns in order to empower others to defend themselves and others against abuse on the internet. On a multi-faceted basis, with both legislative reform, international cooperation, and technological solutions, we can create better means of fighting cyberbullying and online harassment and ultimately a safer digital world for everyone.

By filling in these gaps, the law can more effectively deal with the complexities of contemporary digital interactions and shield people from the ruinous effects of online harm.

REFERENCES

- [1]. Pew Research Center. (2018). "The State of Online Harassment." Retrieved from <https://www.pewresearch.org>
- [2]. United States Congress. (2009). "Megan Meier Cyberbullying Prevention Act." Retrieved from <https://www.congress.gov>
- [3]. European Parliament. (2016). "General Data Protection Regulation (GDPR)." Official Journal of the European Union. Retrieved from <https://gdpr.eu>
- [4]. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, India. Ministry of Electronics and Information Technology, Government of India. Retrieved from <https://meity.gov.in>
- [5]. Australian Government. (2015). "Enhancing Online Safety Act 2015." Retrieved from <https://www.legislation.gov.au>
- [6]. United States Congress. (1996). "Communications Decency Act, Section 230." Retrieved from <https://www.congress.gov>
- [7]. Council of Europe. (2001). "Convention on Cybercrime." Retrieved from <https://www.coe.int>
- [8]. American Civil Liberties Union (ACLU). (2020). "Section 230 and Free Speech." Retrieved from <https://www.aclu>
- [9]. Shaw, M. (2020). "The Limits of Section 230: Holding Platforms Accountable for Harmful Content." *Harvard Journal of Law and Technology*, 33(2), 255-274.

⁸American Civil Liberties Union (ACLU). (2020). "Section 230 and Free Speech." Retrieved from <https://www.aclu>



- [10]. Livingston, J. (2019). "International Cyberbullying Laws: A Comparative Analysis." *Journal of Internet Law*, 22(6), 23-47.
- [11]. Hinduja, S., & Patchin, J. W. (2018). "Cyberbullying: An Update and Synthesis of the Research." Cyberbullying Research Center. Retrieved from <https://cyberbullying.org>
- [12]. Sweeney, L. (2020). "Technological Solutions for Cyberbullying Prevention." *Journal of Digital Safety*, 14(3), 112-131.

