International Journal of Enhanced Research in Educational Development (IJERED)
ISSN: 2320-8708, Vol. 13 Issue 3, May-June, 2025

An Assessment of Legal Mechanisms to Combat Online Harassment of Women and Children

Kanchan Kunwar[1], Dr. Narendra Kumar Singh[2]

[1,2]Department of Law, Kalinga University, Raipur, Chhattisgarh

ABSTRACT

Unfortunately, cyberbullying has also increased with internet use, with women and children bearing the brunt of this trend. The psychological and social effects of cyberstalking, cyberbullying, sexual exploitation, and hate speech are examined in this research, which also provides a critical assessment of these types of online harassment. The Indian Penal Code, the Information Technology Act, 2000, and the Protection of Children from Sexual Offences (POCSO) Act are some of the important legislations that are examined in this evaluation of the current legal framework in India's efforts to combat online abuse. In order to comprehend the difficulties in enforcement, the function of institutional mechanisms such as cybercrime sections within police departments, interventions by the courts, and reporting portals is examined. Also included in the article are some of the loopholes, such as victims not being reported enough, complicated jurisdictions, and perpetrators' ability to remain anonymous online. To have a better understanding of what works, it is helpful to compare different international legal regimes. The report emphasizes the need of raising awareness, improving enforcement capabilities, and fostering international collaboration in order to ensure that women and children in India who experience online harassment get the protection and justice they deserve, even if the country has progressive legislation in place.

Keywords: Online Harassment, Cyber Law, Gender-Based Violence, Child Protection, Digital Safety.

INTRODUCTION

Worldwide, people are now able to communicate, connect socially, and share knowledge much more quickly than in the past because to the proliferation of digital technology and the internet. In spite of all these positive aspects, the internet has also become a haven for sexual harassment, assault, and other types of abuse, especially against women and children. There are significant psychological, social, and legal ramifications to the growing issue of online harassment, which includes a wide range of behaviors such as cyberbullying, stalking, trolling, and doxxing, as well as more extreme types of gender-based violence such as sexual harassment and exploitation. The social position of women and children, together with their frequently restricted access to protective services, makes them disproportionately vulnerable to virtual violence. Their susceptibility is amplified by the anonymity and widespread reach of digital platforms, which makes it difficult to adequately monitor, deter, and prosecute offenders.

As digital crimes have become more widely acknowledged, the legal frameworks aimed at combating online harassment have also developed. Online harassment, sexual exploitation, and abuse have been criminalized in some countries, including India, the US, and the EU, among others. These laws aim to safeguard children and women from such abuse. Online harassment, cyber stalking, and the dissemination of obscene information are criminalized in India under the terms of the Information Technology Act, 2000 (IT Act) and the Indian Penal Code (IPC). Specialized legislation, such as the POCSO Act of 2012, further protects minors from sexual assaults committed online. The digital domain has no geographical bounds, and legal frameworks often fall behind the ever-changing strategies utilized by criminals, making enforcement of these laws very difficult.

Finding a middle ground that protects victims' rights while still allowing for free speech online is a significant difficulty in the fight against internet harassment. A well-balanced legal response is necessary to penalize harassment and abuse without stifling free expression or invasion of privacy. Additionally, the investigation and prosecution of cybercrimes necessitates the development of technical competence, which in turn necessitates the strengthening of capacities within the judicial system, regulatory organizations, and law enforcement. Social shame, ignorance of their rights, and difficulty obtaining justice are additional obstacles that victims confront, particularly children and women.

The purpose of this evaluation is to determine how well current legal safeguards protect children and women against cyber bullying. It investigates whether the existing legal frameworks, institutional responses, and procedural safeguards are sufficient to provide victims with protection and compensation. Given the centrality of digital platforms and intermediaries in online communication, the research also investigates their role in reacting to and avoiding harassment.

Because international collaboration is essential in combating cybercrimes, it also takes into account the interaction between national laws and human rights norms. The goal of this study is to help create stronger regulations that are more adaptable to technology by identifying the areas where laws are lacking and where they are strong.
The importance of community involvement, education, and awareness efforts in reducing online harassment should not be understated, nor should the significance of legislative actions. A complete approach must include sensitizing the public and government, as well as empowering women and children with digital literacy and safe online habits. Preventing, protecting, prosecuting, and rehabilitating victims of online harassment are all necessary parts of the fight against this kind of behavior. Findings from this study highlight the need for new laws, more enforcement, and a coordinated effort by many groups working to protect children and women online. These groups include governments, non-profits, internet corporations, and international organizations.

What Is Cyber Harassment And Bullying?
In their lifetime, an estimated one-third of the world's women will be victims of sexual or physical abuse (WHO 2021). Equally troubling is the alarming increase in cyber bullying and harassment directed at women and girls. For instance, research indicates that 73% of women in the EU have experienced online harassment or assault. Cyber stalking and harassment affect women at a much higher rate than males, according to a German study of over 9,000 internet users (ranging in age from 10 to 50). Women are the targets of an estimated 95% of online aggressiveness, harassment, abusive language, and demeaning pictures, according to the United Nations (UN). Violence against women and girls (VAWG) has only become worse due to the COVID-19 epidemic. While the real world grew less secure for women and girls during the pandemic because to the significant rise in intimate partner violence, the online world became even more deadly for them due to the increasing dependence on technology and virtual communication. For example, allegations of cyberbullying and abuse in Australia have surged 50% since the COVID-19 pandemic began. An extra 58% of females and girls had direct encounters with cyberbullying in 2020, according to Plan International research that touched on 22 countries.

The rapid development of ICT has meant that new terms describing forms of online violence against women are constantly appearing in the field. Given the multifaceted nature of cyberbullying, it's possible that more conventional concepts of violence are inadequate. Online violence against women will continue to evolve and take new forms as digital spaces and technologies, such as AI, continue too rapidly advance. Traditional legal protections for women may not be enough in the face of sexual harassment that takes place via electronic means such as cell phones, the web, social media, and email. The confused interchangeability of terminology like cyber violence, cyber harassment, digital violence, and online violence adds to the problem. But cyber or online violence is a catch-all word for a wide range of behaviors; it includes things like doxing, nonconsensual pornography, revenge porn, faming, cyber stalking, cyber harassment and bullying, online gender-based hate speech, faming, image-based sexual abuse, and many more (table 1). Anyone from close friends and family to strangers in a casual online relationship might engage in such harmful actions. When people commit, aid, or exacerbate any form of gender-based violence against a woman, either because she is a woman or because of the disproportionate impact that this form of violence has on women, it is generally considered to be online violence against women.

This includes acts that take place on or around the internet, social media platforms, email, and mobile phones and smartphones. Cyberbullying, a kind of cyber violence, is defined as the intentional use of electronic communication channels (email, instant messaging, etc.) to harass, threaten, intimidate, or otherwise negatively impact a specific individual. Any unwelcome sexually-oriented verbal or nonverbal behavior that occurs online and has the intent or consequence of making another person feel threatened, aggressive, degraded, humiliated, or offensive is considered cyber sexual harassment. Sending unsolicited, insulting, or sexually explicit emails or messages and making improper, offensive approaches on social networking sites or internet chat rooms are specific actions that may be considered online sexual harassment. Economic, social, and bodily damages are all possible outcomes of cyberbullying and harassment. The European Union commissioned research in 2021 that put the price tag of cyber violence anywhere between €49.0 and €89.3 billion. More than half of these projected expenses are attributable to the monetary worth of the loss in terms of quality-of-life, in addition to labor market implications, health care expenditures, and legal fees.

Some of the social effects include a decline in women's economic independence and online visibility, as well as a decrease in women's access to and participation in digital communities. Some may be scared to seek out popular figures like politicians, artists, journalists, or activists because of the prevalence of online harassment against women in these fields. Last but not least, acts of online aggression often follow or precede their offline counterparts. Seventy percent of victims of cyberstalking and harassment have also been victims of intimate relationship abuse, according to the research.

Existing Gaps In The Policies And Legislation
Despite the development of numerous statutes aimed at curbing cybercrimes, existing legal and policy frameworks in India display significant deficiencies in effectively addressing the lived realities of online harassment experienced by women and children. These gaps not only limit the scope of justice but also expose victims to continuous vulnerabilities in the digital ecosystem.

Paternalistic Legal Attitudes and Gender-Blind Frameworks
The current legal system often operates from a paternalistic mindset rooted in moral policing rather than victim-centric justice. This attitude is evident in the prioritization of morality over individual autonomy and rights. For instance, in the aftermath of viral videos—such as one showing women playing Holi in the Delhi Metro—public and legal discourse centered on notions of vulgarity and morality, ignoring the central issue of consent and digital safety. Such reactions demonstrate a broader societal insensitivity toward the issue of online gender-based violence. Additionally, the push for gender neutrality in laws has inadvertently diluted protections for women by ignoring the disproportionate and gendered nature of digital abuse. Women, especially from marginalized communities, require focused legal safeguards that account for intersectional vulnerabilities.

Narrow Definition of Privacy Violations in the IT Act
The Information Technology Act, 2000, while being the primary legislation governing cybercrimes in India, presents a restrictive and outdated understanding of privacy violations. Section 66E of the Act criminalizes the capture and transmission of private images of body parts without consent; however, this definition fails to encapsulate the wide array of digital privacy breaches that occur today. Online invasions of privacy through non-consensual surveillance, data leaks, doxxing, deepfake pornography, and unauthorized use of personal images and conversations are not adequately addressed within the Act. The legislation's narrow scope leaves victims of these newer and more sophisticated forms of cyberviolence without recourse.

Ambiguities around Consent and Enforcement of the DPDP Act, 2023
Consent remains a core element in determining the legality of data sharing and online actions. However, in the context of online abuse, determining whether victims consented to the circulation of images or information can be fraught with complexity. In many cases, images may be shared under coercion, manipulation, or with revoked consent, scenarios the current legal mechanisms struggle to address adequately. The recently introduced Digital Personal Data Protection Act, 2023 (DPDP) holds potential in this regard, especially with the rise of deepfakes and AI-enabled identity breaches. Nonetheless, it is still in its infancy and lacks clear guidelines on enforcement, penalties, and jurisdiction, especially in the context of gendered harms.

Algorithmic Biases and Data Mining by Digital Platforms
Internet platforms frequently mine users' data without informed consent, facilitated by lengthy and complex terms and conditions that users rarely understand or fully consent to. These platforms' algorithms have been shown to perpetuate racist, sexist, and casteist biases, reinforcing harmful stereotypes and targeting users with discriminatory content. However, India's legal system has yet to evolve mechanisms to hold these platforms accountable for algorithmic harms. There is a pressing need for transparency and regulation concerning how platforms collect, use, and profit from user data, particularly when such practices lead to targeted harassment or exploitation.

Unclear Accountability: State vs. Non-State Actors
Another critical gap is the ambiguity in assigning responsibility for cybercrimes between state and non-state actors. Legal provisions often fail to identify or regulate the roles of non-state actors in orchestrating harassment campaigns. A glaring example includes the "Bulli Bai" and "Sulli Deals" cases, where Muslim women were virtually "auctioned" in a targeted, misogynistic campaign. Despite public outrage and media coverage, the legal system struggled to deliver swift justice due to the absence of robust frameworks dealing with such coordinated digital hate crimes. Moreover, laws do not mandate stringent monitoring mechanisms for platforms where such crimes occur.

Paternalistic Safety Apps and Tokenistic Solutions
In response to increasing online violence, various "safety apps" have been developed claiming to protect women online. However, these technologies often adopt a paternalistic approach—offering surveillance rather than empowerment—and rarely address the structural causes of digital gender-based violence. They also lack integration with law enforcement or judicial mechanisms, limiting their usefulness in ensuring justice or deterrence.

Procedural Barriers and Victim Retraumatization
Women and children face multiple barriers when seeking redress for online violence. These include prolonged delays in investigations, low conviction rates, and complex legal procedures that are often not survivor-friendly. Victims frequently lack legal and digital literacy, making navigation through justice systems intimidating. Fear of character assassination, social stigma, and gender-based courtroom stereotypes further dissuade victims from filing complaints. The justice process, instead of offering relief, can often be retraumatizing due to insensitive questioning and lack of support structures.

Lack of Police Training and Sensitization
Many studies have highlighted the inadequacy of police training in dealing with cybercrimes, especially those involving gender-based digital abuse. Law enforcement officials often misuse or misunderstand cyber laws, as seen in continued bookings under Section 66A of the IT Act even after it was struck down by the Supreme Court in the Shreya Singhal v. Union of India (2015) case. This persistent misapplication reveals a serious gap in legal knowledge,

indicating that legal reforms are ineffective without simultaneous reforms in training and institutional awareness. Sensitization programs on gender, digital rights, and psychological impacts must be mainstreamed into police training curricula.

Inadequate Resources and Infrastructure for Cybercrime Enforcement
The enforcement infrastructure for tackling cybercrime remains weak and under-resourced. Cyber cells are unevenly distributed, underfunded, and lack the technical expertise and manpower needed to address the growing sophistication of online crimes. There is an urgent need to increase public investment in cyber forensic infrastructure, recruit trained personnel, and ensure 24/7 accessibility of reporting systems.

Legal Protection Across The Globe To Protect Women And Children From Cyberviolence
The Anonymity and Complexity of Cybercrime
Cybercrime, unlike conventional crimes, thrives on anonymity. Perpetrators often exploit digital tools such as VPNs, fake accounts, and encrypted communications to mask their identity. This anonymity allows offenders to breach moral, ethical, and legal boundaries without immediate consequences. The digital environment complicates law enforcement efforts due to the lack of physical evidence, difficulty in tracking locations, and jurisdictional limitations. As online crimes become more technologically sophisticated, law enforcement agencies are increasingly challenged by opaque and decentralized digital systems.

Global Surge in Online Abuse Against Women and Children
The accessibility and affordability of internet-enabled devices have led to the rapid increase of online violence, especially targeting women and children. These vulnerable groups face cyberstalking, online grooming, image-based sexual exploitation, hate speech, and threats. The increasing prevalence of such abuse calls for urgent legal reforms, yet many nations are unprepared to handle the evolving nature of these digital threats.

International Legislative Landscape: Gaps and Variations
According to a World Bank analysis, only 30% of nations have laws specifically addressing cyber harassment. This means that more than half of the world's female population remains without adequate legal protection. Of the 190 countries surveyed, only 53 have criminalized cyber harassment, and merely 19 have established clear procedures for reporting and prosecuting such crimes. This stark disparity underscores the global neglect of gender-sensitive digital safety.

Legislative Initiatives in African Nations
Some African countries have taken proactive steps in tackling cyberviolence.

- **South Africa's Cybercrimes Act (2020)** includes explicit provisions against cyber harassment, threats, and image-based abuse.
- **Nigeria's Cybercrimes Act (2015)** criminalizes various online offenses, including threats, identity theft, and child exploitation.
- **Uganda** has incorporated cyberbullying and hate speech provisions into its penal code. These laws are critical first steps, although challenges in enforcement and awareness persist.

European Approaches: Platform Regulation and Gender Neutrality
European countries display a mixed approach—some, like Germany, have enacted robust legislation such as the NetzDG law, which compels social media platforms to remove illegal content within 24 hours. Others use gender-neutral laws to address cybercrime broadly, though this may obscure the gendered realities of online violence. While the EU emphasizes data protection and privacy rights through laws like GDPR, more targeted strategies are needed to address gender-specific harms online.

The United States: Child Protection and Legal Controversies
In the U.S., various laws like the Violence Against Women Act (VAWA) and COPPA aim to protect women and children online. Federal laws penalize child sexual abuse material and online grooming, and some states have specific laws against cyberstalking and revenge porn. However, the controversial Section 230 of the Communications Decency Act continues to shield tech companies from liability for user-generated content, raising concerns over platform accountability in enabling cyberviolence.

Lack of Global Coordination and Binding Instruments
Despite some international instruments like the Budapest Convention on Cybercrime, there is no unified, binding global framework to protect women and children from cyberviolence. United Nations resolutions and soft law instruments provide recommendations but lack enforcement mechanisms. The absence of global consensus and cooperation hinders the cross-border investigation and prosecution of cybercrimes.

Emerging Technologies and Legal Voids
The rise of artificial intelligence, deepfake technology, and facial recognition tools has introduced new forms of digital abuse. AI-generated non-consensual sexual content, manipulated videos and identity theft have emerged as threats, with minimal legal recognition or regulation. Most legal systems have yet to evolve to address these advanced forms of cyberviolence, leaving victims without legal protection.

Neglect of Human Rights in Technological Advancements
New technologies are often developed without adequate consideration for their social impact, especially on marginalized communities. The rights and safety of women and children are frequently sidelined in the race for innovation. As a result, the expansion of the digital space has created new avenues for exploitation and abuse, with little regard for establishing safeguards or accountability.

The Need for a Gender-Sensitive, Global Legal Framework
To combat cyber violence effectively, there must be a coordinated international effort to develop gender-sensitive legal frameworks that are adaptable to technological advancements. These frameworks should be victim-centered, proactive, and enforceable across jurisdictions. Legal reforms must be supported by capacity-building initiatives for law enforcement, mandatory platform accountability, and robust mechanisms for redress and psychological support.

The Legal Matrix Regulating Cybercrimes Against Women In India
In recent years, there has been a disturbing increase in cybercrimes targeting women. The National Crime Record Bureau recorded an 11% increase in events reported in 2022 compared to 2021 in their report issued in December 2023. As reports of domestic violence against women and children rose throughout the epidemic, so did the variety and scale of cybercrime. Cybercrime has become more common as the number of people using mobile phones, tablets, laptops, desktops, and other electronic devices for work, school, play, and financial transactions has increased.

The Indian Penal Code (IPC) or the Information Technology Act (IT Act) of 2000 has the legal framework to address cybercrimes in India. There is a lack of legislation that targets cyber assault against women. When a male engages in sexually harassing behavior, such as asking a woman for a sexual favor, forcing her to see pornographic material against her will, or making sexually suggestive comments, he is subject to the penalties outlined in Section 354A of the Indian Penal Code. A woman is guilty of voyeurism if she consents to the taking or dissemination of photographs of her engaging in a private act without her knowledge or consent, as found in Section 354C of the Indian Penal Code. Cyberstalking, which includes the act of following a woman about via email or the internet, is punishable under Section 354D of the Indian Penal Code. When necessary, other sections of the IPC may be used, such as those pertaining to criminal defamation, extortion, cheating, criminal intimidation, and insults to women's modesty.

Cyber fraud, email spoofing, sending threatening communications via email, hacking, tampering, privacy and confidentiality breaches, publishing forged digital signatures, and falsification of electronic documents are among crimes that the IT Act tackles. The laws that were put in place in 2013 designate an administrative agency as the Computer Emergency Response Team. Its job is to gather, analyze, and share information about security issues. Cybersecurity incident reporting requirements will be revised in 2022. Additionally, identity theft is punishable under Section 66C of the IT Act. As stated in this section, it is considered a crime to use the password or electronic signature of another person. Violating someone's right to privacy is punishable under Section 66E. Publication, transmission, or instigating transmission of pornographic material is expressly forbidden under Section 67A. Penalties for violations of privacy and secrecy are outlined in Section 72. Thus, the IT Act offers a patchwork solution and lacks rules tailored to tackle crimes perpetrated by certain genders.

In addition, cases involving online violence may be subject to laws such as the Protection of Sexual Harassment Act, 2013, which acknowledges harassment of women in the workplace, the POCSO Act, 2012, which governs sexual offenses perpetrated against children, and the Indecent Representation of Women (Prohibition) Act, 1986, which regulates the portrayal of women in advertisements, publications, and other formats. Problems arise, however, when trying to put these rules into practice. To illustrate the point, the primary goal of the Indecent Representation of Women Act is to safeguard public morals, not to ensure the protection of women. Furthermore, no particular measures have been passed to address the changing scenario, even though cybercrimes against women are on the rise.

National Cyber Security Policy 2023
'To develop a safe and resilient cyberspace for individuals, industry, and government' was the objective behind the 2013 National Cyber Security Policy. Responding to cyber-attacks and protecting information and infrastructure are its primary goals. Protective measures for 2023 have been updated to better react to cyber threats, reduce vulnerabilities, and stop malware assaults. Cybercrime monitoring and easing compliance with cyber security measures are the primary goals of this strategy. In order to guarantee that this policy eradicates online violence and empowers women who utilize technology, it must be examined from a feminist viewpoint. Launched in 2018, the Cyber Crime Prevention against Women and Children (CCPWC) project aims to address cybercrimes perpetrated against women and children in India. The Cyber Crimes Reporting and Analysis Center (CCPWC) reports crimes, sets up forensic laboratories, and run

awareness initiatives. A number of supplementary steps, however, have been proposed by the National Commission for Women. These include establishing a dedicated online crime reporting unit for women, keeping tabs on online crimes, enhancing investigative capabilities, and capacity development. Anyone may use the National Cybercrime Reporting Portal to anonymously report cybercrimes against children and women. I4C has also been set up as a central organization to combat cybercrime. The ground-level effect of these regulations on the issue of rising cybercrime against women is yet not apparent.

The non-governmental organization Prajwala also expressed concern in a 2015 petition it sent to the Supreme Court over the widespread distribution of pornographic and violent content online. Notifications were sent to Google, Microsoft, Yahoo!, Facebook, and WhatsApp in response to this letter. In March 2017, the Court ordered the formation of a committee to investigate potential technical solutions to safeguard victims' identities and reputations and stop the spread of these recordings for the sake of public interest. The need of establishing a Central Reporting Mechanism to bolster law enforcement was acknowledged by the Committee. Businesses could help strengthen law enforcement authorities' capabilities by providing technology assistance. Data Protection (Intermediary Standards and Digital Media Ethics Codes) Rules, 2021 were ordered by the court to be enforced. To prevent child injury and privacy invasion, these Guidelines lay forth the ground rules for social media intermediaries to follow. In addition, a system is being established to address complaints of gender-based harassment. Still, little was done to bridge the digital gap. Additionally, there is a pressing need for further feminist-informed legislative reforms to end cyber violence against women in all its forms.

CONCLUSION

The pressing need for efficient legal procedures adapted to the digital era has been highlighted by the growing incidence of cyber bullying affecting minors and women. Although India has made great strides with laws like the IT Act and the POCSO Act, there are still problems with awareness, enforcement, and technology adoption. This evaluation shows that laws aren't enough on their own; other measures like capacity-building, victim care, and coordination between stakeholders are needed. Because cybercrime may happen anywhere in the world, there has to be more international collaboration and legal harmonization. When it comes to reacting to and preventing harassment on their services, digital platforms also need to step up their game. To guarantee that children and women may use the internet securely and with respect, we need a comprehensive strategy that incorporates strong legislative frameworks, effective enforcement, education, and community involvement. Both vulnerable populations and the basic liberties and rights enjoyed by all members of a digital society may be safeguarded by enhancing these systems.

REFERENCES

[1]. Chakan and M. F. Millenio, “Protection of Cyber bullying Victims in Indonesia (An Overview of Law and Victimology),” Semarang State University Undergraduate Law and Society Review, vol. 3, no. 1, pp. 1–26, 2023.
[2]. S. Ebube, “The Role of Legal Frameworks in Addressing Online Hate Speech and Cyberbullying,” American Journal of Law and Policy, vol. 1, no. 1, pp. 13–24, 2023.
[3]. N. Hussain, A. Khan, L. A. Chandio, and S. Oad, “Individual criminal responsibility for the crime of aggression: the role of the ICC's Leadership Clause,” Pakistan Journal of Humanities and Social Sciences, vol. 11, no. 1, pp. 223–232, 2023.
[4]. A. Khan, N. Hussain, and S. Oad, “The Rome Statute: A Critical Review Of The Role Of The SWGCA In Defining The Crime Of Aggression,” Pakistan Journal of International Affairs, vol. 6, no. 1, 2023.
[5]. Khan and M. A. H. S. Jiliani, “Expanding the boundaries of jurisprudence in the era of technological advancements,” IIUMLJ, vol. 31, no. 2, pp. 393–410, 2023.
[6]. Khan, K. Javed, A. S. Khan, and A. Rizwi, “Aggression and individual criminal responsibility in the perspective of Islamic law,” Competitive Social Science Research Journal, vol. 3, no. 1, pp. 35–48, 2022.
[7]. Khan, S. H. Bhatti, and A. Shah, “An overview on individual criminal liability for crime of aggression,” Liberal Arts and Social Sciences International Journal (LASSIJ), vol. 5, no. 1, pp. 432–442, 2021.
[8]. Khan, S. Amjad, and M. Usman, “The Role of Customary International Law in Contemporary International Relations,” International Review of Social Sciences, vol. 8, no. 08, pp. 259–265, 2020.
[9]. S. Mahmood, “Are Cyberbullying Interventions and Criminal Law Prevention Effective? (A Review of Cyberbullying Legislation in Iraq),” PalArch’s Journal of Archaeology of Egypt/Egyptology, vol. 17, no. 7, pp. 16983–16998, 2020.
[10]. T. K. Chan, C. M. Cheung, and R. Y. Wong, “Cyberbullying on social networking sites: The crime opportunity and affordance perspectives,” Journal of Management Information Systems, vol. 36, no. 2, pp. 574–609, 2019.
[11]. L. Franco and K. Ghanayim, “The criminalization of cyberbullying among children and youth,” Santa Clara Journal of International Law, vol. 17, no. 2, 2019.
[12]. A. El Asam and M. Samara, “Cyberbullying and the law: A review of psychological and legal challenges,” Computers in Human Behavior, vol. 65, no. 2, pp. 127–141, 2016.

[13]. M. Seralathan, "Making the time fit the crime: Clearly defining online harassment crimes and providing incentives for investigating online threats in the digital age," Brooklyn Journal of International Law, vol. 42, no. 5, pp. 425–460, 2016.
[14]. Kerstens and S. Veenstra, "Cyber bullying in the Netherlands: A criminological perspective," International Journal of Cyber Criminology, vol. 9, no. 2, pp. 144–158, 2015.
[15]. S. Kift, M. Campbell, and D. Butler, "Cyberbullying in social networking sites and blogs: Legal issues for young people and schools," Journal of Law, Information and Science, vol. 20, no. 1, pp. 60–79, 2009.