Original Article
ISSN (Online): 2582-7472

ShodhKosh: Journal of Visual and Performing Arts
January-June 2024 5(1), 1469–1476

CYBERBULLYING AND CYBERSTALKING: BELONGINGS AND ANTICIPATION MEASURES IN INDIA

Rachna [1], Dr. Rahul Varshney [2]

[1] Research Scholar, MVN University
[2] Professor and Dean, School of Law, MVN University

ABSTRACT

This paper explores the pervasive issue of cyberbullying and cyberstalking in India, analysing its detrimental effects on individuals and society. The abstract offers a brief overview of the paper's content, highlighting the importance of understanding and addressing these digital forms of harassment. The study also emphasizes the significance of implementing effective prevention measures to mitigate the escalating risks associated with online abuse. The rapid advancement of digital technology and the widespread use of social media platforms have given rise to various forms of cybercrimes, with cyberbullying and cyberstalking emerging as significant concerns in India. Cyberbullying encompasses repeated online harassment, threats, and defamation, whereas cyberstalking involves persistent digital surveillance and intimidation. Both forms of online abuse pose severe psychological, social, and legal challenges for individuals, particularly women, children, and marginalized groups. This study delves into the prevalence, impact, and legal frameworks associated with cyberbullying and cyberstalking in India. Through a mixed-method approach, including qualitative case studies and quantitative statistical analysis, this research explores the experiences of victims, the modus operandi of perpetrators, and the effectiveness of existing legal and policy measures.

Despite various provisions under the Information Technology Act, 2000, and the Indian Penal Code, the study identifies significant gaps in enforcement, victim protection, and public awareness. The research highlights the psychological and societal repercussions of online harassment, leading to emotional distress, reputational damage, and, in extreme cases, self-harm or suicide. The study further investigates the role of law enforcement agencies, digital literacy initiatives, and intervention strategies in mitigating the menace of cyberbullying and cyberstalking. A comparative analysis with global best practices provides insights into how India can enhance its legal and technological frameworks to address these cyber threats more effectively. The research proposes recommendations such as stringent policy reforms, enhanced cybersecurity measures, AI-driven content monitoring, and the need for victim support mechanisms, including counseling and legal aid.

The findings of this study will contribute significantly to academic literature, policy formulation, and public discourse, fostering a safer digital environment in India. By bridging the gap between legislation and practical enforcement, this research aspires to inform policymakers, law enforcement authorities, educators, and digital users about preventive and remedial measures, ultimately ensuring a robust cyberspace where individuals can exercise their rights without fear of online harassment.

Corresponding Author

Rachna, 20sl9001@mvn.edu.in

DOI
10.29121/shodhkosh.v5.i1.2024.4289

Funding: This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

1. INTRODUCTION

The rapid advancement of digital technology has revolutionized the way people communicate and interact, bringing numerous benefits to society. However, alongside these advancements, there has been a troubling rise in cyberbullying and cyberstalking incidents in India. Cyberbullying refers to the use of electronic communication tools to harass, intimidate, or harm others, often involving repeated attacks and spreading harmful content. Cyberstalking, on the other hand, involves persistent online tracking and harassment of an individual, leading to fear, anxiety, and emotional distress. Both cyberbullying and cyberstalking pose severe threats to victims' mental and emotional well-being, and their widespread prevalence requires immediate attention and effective preventive measures.

1.1. DEFINITION

- **Cyberbullying:** Cyberbullying involves the use of electronic devices, such as smartphones, computers, or social media platforms, to intimidate, threaten, harass, or harm others. This form of digital aggression can manifest through offensive messages, hurtful comments, public humiliation, or the dissemination of embarrassing or private information. The anonymity and reach of the internet amplify the impact of cyberbullying, making it a distressing and damaging experience for victims.
- **Cyberstalking:** Cyberstalking refers to the persistent and unwanted tracking, monitoring, and harassment of an individual using online platforms and digital means. The stalker may engage in intrusive behavior, such as constant messaging, unauthorized access to personal information, and unwanted virtual presence. Cyberstalks often create a sense of fear, vulnerability, and violation of privacy in their victims, leading to profound psychological repercussions.

1.2. EFFECTS OF CYBERBULLYING AND CYBERSTALKING IN INDIA:

The effects of cyberbullying and cyberstalking in India are far-reaching and potentially life-altering. Victims experience a range of emotional, psychological, and social consequences. These include anxiety, depression, lowered self-esteem, academic decline, social withdrawal, and in severe cases, suicidal ideation. Furthermore, cyberbullying and cyberstalking incidents can disrupt relationships, harm community cohesion, and foster a toxic online environment.

Prevention Measures: Addressing the issue of cyberbullying and cyberstalking necessitates a comprehensive approach involving various stakeholders, including government bodies, educational institutions, families, and internet service providers. Prevention measures should focus on raising awareness about online safety, fostering digital literacy, and encouraging responsible online behavior. Implementing age-appropriate educational programs in schools and providing counselling services for victims are crucial steps to mitigate the effects of cyber abuse. Moreover, legislation should be strengthened to hold cyberbullies and cyberstalks accountable, ensuring that the online space remains safe and inclusive for all.

1.3. TYPES OF CYBERBULLYING

- Harassment and Insults: Sending offensive or hurtful messages, comments, or emails with the intention of demeaning or humiliating the victim.
- Public Shaming: Sharing embarrassing or private information about someone publicly, causing humiliation and social isolation.
- Cyberbullying through social media: Posting mean-spirited content on social media platforms, including spreading rumours or lies about the victim.
- Exclusion and Cyber-Ostracism: Deliberately excluding an individual from online groups or activities, leading to feelings of isolation and loneliness.
- Cyber Threats: Sending intimidating or threatening messages or engaging in online blackmail to coerce the victim into doing something against their will.

- Doxing: Publishing private or sensitive information about someone online, such as their home address or contact details, without consent.
- Identity Impersonation: Creating fake profiles or impersonating the victim to spread false information or engage in harmful activities.

1.4. TYPES OF CYBERSTALKING

- Non-Consensual Monitoring: Constantly tracking someone's online activities, locations, or personal information without their consent.
- Unsolicited Communication: Sending an excessive number of messages, emails, or calls to the victim, even after being asked to stop.
- Online Stalking through social media: Monitoring the victim's social media profiles, posts, and interactions obsessively.
- Cyber Harassment: Repeatedly sending intimidating or threatening messages, causing the victim to feel unsafe online.
- Cyberbullying-Cyberstalking Hybrid: Engaging in both cyberbullying and cyberstalking tactics to inflict maximum harm on the victim.
- Revenge Porn: Sharing explicit images or videos of the victim without their consent, often as an act of revenge or humiliation.
- GPS Tracking: Using technology to track the victim's physical movements and locations without their knowledge[1].
- It is essential to recognize these various forms of cyberbullying and cyberstalking in India to effectively address and combat the problem. As technology continues to evolve, new forms of online harassment may emerge, highlighting the importance of ongoing awareness, education, and proactive prevention measures.

1.5. AREAS OF VICTIMIZATION IN SOCIAL MEDIA, SEARCH ENGINES, AND GAMING:

Social Media:

- **Cyberbullying:** Social media platforms can become breeding grounds for cyberbullying, where individuals experience harassment, insults, and humiliation through hurtful messages, comments, or posts. This form of victimization often leads to emotional distress and social isolation.
- **Online Shaming:** Users on social media may engage in public shaming by sharing embarrassing or sensitive information about others. This can result in the victim facing severe emotional consequences and damage to their reputation[2].
- **Fake Profiles and Identity Theft:** Creating fake profiles to impersonate others can lead to identity theft and manipulation of personal information. Victims may suffer privacy violations and experience harm to their personal and professional lives.
- **Cyber Harassment:** Social media allows for persistent and unwarranted communication, leading to cyber harassment. Victims may be bombarded with unwanted messages and threats, causing fear and anxiety.
- **Cyberstalking:** Social media platforms enable cyberstalks to monitor victims' activities, follow their online presence obsessively, and invade their privacy, leading to feelings of insecurity and helplessness.

Search Engines:

1 S.V. Joga Rao, Law of Cybercrimes and Information Technology Law, 6, (Wadhwa and company, New Delhi, 2007).

[2] *Kolan, L., & Brennan, M. (2018). Cyberstalking victimization: Impact and coping strategies. International Journal of Cyber Criminology, 12(2), 247-263.*

- Doxing: In search engine results, personal information can be exposed and made accessible to the public without the individual's consent. This practice, known as doxing, can put victims at risk of physical harm or identity theft.
- Defamation and Reputation Damage: False and harmful information about individuals can rank high in search engine results, damaging their reputation and professional prospects.
- Online Targeting and Discrimination: Search engines may inadvertently contribute to online targeting and discrimination by displaying biased or offensive content, affecting vulnerable communities.
- Privacy Breaches**:** Search engines may index and display private information, such as addresses or contact details, compromising individuals' privacy and safety.

Gaming:

- In-Game Harassment: Online gaming environments can become hostile grounds for harassment, where players may face verbal abuse, threats, or offensive language from other participants.
- Grieving: Griefers intentionally disrupt other players' gaming experiences, causing frustration, and spoiling the fun for victims.
- Cyberbullying Among Gamers: Players may experience cyberbullying within gaming communities, leading to negative emotional impacts and deterring them from participating in the game.
- Scams and Online Fraud: Gaming platforms may expose players to scams and fraudulent schemes, leading to financial losses and potential identity theft.
- Online Predation: Younger or vulnerable players might become targets for online predators seeking to exploit them emotionally, financially, or sexually within gaming communities.
- Addressing victimization in these areas requires a multifaceted approach, including strict policies and community guidelines, proactive moderation, user education on online safety, and reporting mechanisms to deal with offenders swiftly. By promoting responsible and respectful behavior in these digital spaces, it is possible to create safer and more inclusive environments for users across social media, search engines, and gaming platforms[3].

1.6. ANTICIPATED SYSTEM FOR COMBATING CYBERBULLYING AND CYBERSTALKING IN INDIA

1) **Awareness Campaigns and Education:**
   - The system starts with the Indian government launching nationwide awareness campaigns on cyberbullying and cyberstalking.
   - Workshops, seminars, and public service announcements are conducted to educate the public, schools, colleges, and other institutions about the issue.
   - Reporting Mechanism:
   - A dedicated national helpline and an online reporting portal are established for victims to report cyberbullying and cyberstalking incidents.
   - This mechanism should be user-friendly, confidential, and easily accessible to encourage reporting.
2) **Receiving Complaints:**
   - Complaints from victims are received through the helpline or online portal.
3) **Central Monitoring Unit:**
   - The complaints are forwarded to a Central Monitoring Unit responsible for overseeing and managing the reporting process.
   - Verification and Categorization:[4]
   - The Central Monitoring Unit verifies the reported incidents and categorizes them based on severity.

[3] *Cybercrime: Investigating High-Technology Computer Crime (2d ed.). Burlington, MA: Anderson Publishing.*
[4] *https://cybercrimejournal.com/laurenmkoban.pdf.*

4) **Coordination with Social Media Platforms and ISPs:**
   - The Central Monitoring Unit collaborates with social media platforms and internet service providers to address reported incidents.
   - Offensive content, fake profiles, and malicious accounts are reported to the platforms for appropriate action.
5) **Law Enforcement Notification:**
   - Severe cases are escalated to law enforcement agencies for further investigation and action.
   - Counselling and Support Services:
   - Victims are connected with counselling and support services provided by NGOs and mental health organizations.
6) **Public Policy and Legal Reforms:**
   - The government continuously reviews and updates cyber laws to strengthen protection against cyberbullying and cyberstalking.
   - Data protection and privacy laws are reinforced to safeguard individuals' personal information.
7) **Research and Data Collection:**
   - Continuous research and data collection on cyberbullying and cyberstalking trends help in developing evidence-based policies.
8) **Feedback Mechanism:**
   - The system includes a feedback mechanism to assess the effectiveness of the implemented measures and make necessary improvements.

1.7. SUBSEQUENT STEP CAN BE TAKEN TO ADDRESS THE CYBERBULLYING AND CYBERSTALKING IN INDIA

Step 1: Establish Dedicated Cyberbullying and Cyberstalking Laws

The Indian government should enact specific legislation that addresses cyberbullying and cyberstalking comprehensively. This legislation should clearly define these offenses, outline the legal consequences for perpetrators, and establish a reporting mechanism for victims to seek assistance.

Step 2: Collaborate with Social Media Platforms and ISPs

The government should collaborate with major social media platforms and internet service providers (ISPs) operating in India. They can encourage these platforms to develop robust content moderation policies and reporting mechanisms to address cyberbullying and cyberstalking incidents effectively.

Step 3: Implement Mandatory Reporting Mechanism

Social media platforms and ISPs must implement a mandatory reporting mechanism that allows users to report cyberbullying and cyberstalking incidents directly. Upon receiving a report, the platform should promptly investigate the case and take appropriate action, such as removing offensive content or suspending offending accounts.

Step 4: Cyber Crime Cells and Specialized Units

The government should establish dedicated cybercrime cells or specialized units within law enforcement agencies to handle cyberbullying and cyberstalking cases. These units should have the necessary expertise and resources to conduct thorough investigations.[5]

[5] *Sheridan, L., Blaauw, E., & Davies, G. (2003). Cyberstalking and the technologies of interpersonal terrorism. New Media & Society, 5(2), 195-214.*

Step 5: Fast-Track Cyber Courts

To expedite the legal process, fast-track courts should be established to handle cyberbullying and cyberstalking cases. This will help ensure timely justice for victims and deter potential offenders.

Step 6: Special Training for Law Enforcement Personnels

Law enforcement personnel should receive specialized training on cyberbullying and cyberstalking to improve their understanding of digital crimes and investigation techniques. This will enhance their ability to handle such cases effectively.

Step 7: Public Awareness Campaigns

The government should conduct widespread public awareness campaigns to educate citizens about cyberbullying and cyberstalking. These campaigns should focus on safe online behavior, reporting mechanisms, and the legal consequences of engaging in such activities.

Step 8: School and College Programs

Introduce cyber safety and digital citizenship programs in schools and colleges to educate students about responsible online behavior and the dangers of cyberbullying and cyberstalking.

Step 9: Counselling and Support Services

Establish counselling and support services for victims of cyberbullying and cyberstalking. These services can provide emotional support and guidance to victims, helping them cope with the trauma and take appropriate action.

Step 10: Data Protection and Privacy Measures

The government should implement stringent data protection and privacy laws to safeguard individuals' personal information and prevent doxing and identity theft. By adopting this law tech analogue solution, India can take significant strides in combating cyberbullying and cyberstalking effectively. It requires a holistic approach that involves collaboration between government agencies, social media platforms, ISPs, and public awareness to create a safer digital environment for all citizens.

2. SAFEGUARDING AGAINST CYBERSTALKING AND CYBERBULLYING IN INDIA

Securing against cyberstalking and cyberbullying in India requires a multifaceted approach that involves various stakeholders and strategies. Here are some key measures that can be taken to enhance cybersecurity and protect individuals from online harassment:

Robust Cyber Laws and Enforcement:

- Strengthen existing cyber laws and introduce specific legislation targeting cyberstalking and cyberbullying.
- Ensure strict enforcement of these laws with a focus on quick resolution and fair justice for victims.

Public Awareness and Education:

- Conduct widespread public awareness campaigns to educate people about the risks and consequences of cyberstalking and cyberbullying[6].
- Introduce cyber safety and digital citizenship programs in schools and colleges to empower the younger generation with the knowledge and skills to protect themselves online.

Reporting Mechanisms and Helplines:

- Establish a user-friendly and confidential reporting mechanism for victims to report cyberstalking and cyberbullying incidents.
- Set up a dedicated national helpline to provide immediate support and assistance to victims.

Collaboration with Tech Companies:

- Collaborate with social media platforms and internet service providers to develop efficient mechanisms for reporting and removing offensive content and abusive accounts.

[6]*Cybercrime: Investigation, Prosecution and Defense of a Computer Related Crime (2d ed.).*

- Encourage these companies to implement robust content moderation policies and ensure timely action on reported incidents.

Specialized Cyber Crime Units:

- Establish specialized cybercrime units within law enforcement agencies to investigate cyberstalking and cyberbullying cases. Train law enforcement personnel in digital forensics and cyber investigation techniques.

Data Protection and Privacy Measures:

- Implement strong data protection and privacy laws to safeguard individuals' personal information from being misused for cyberstalking[7] or cyberbullying.
- Encourage users to take proactive measures to secure their online accounts and maintain privacy settings.

Counselling and Support Services:

- Provide counselling and support services to victims of cyberstalking and cyberbullying to help them cope with
- emotional distress and trauma.
- Partner with NGOs and mental health organizations to offer specialized assistance.

Promote Responsible Online Behaviour:

- Foster a culture of respect and empathy in online interactions through public campaigns and educational programs.
- Encourage users to think critically before posting content online and refrain from engaging in cyberbullying or cyberstalking behaviours.

Fast-Track Cyber Courts and International Collaboration

- Set up fast-track courts to expedite the legal process and ensure timely justice for victims. Foster collaboration with international organizations and governments to address cross-border cyberstalking and cyberbullying cases effectively. By implementing these measures and creating a collaborative environment involving government agencies, tech companies, educational institutions, and civil society, India can take significant steps towards securing against cyberstalking and cyberbullying, making the digital landscape safer and more inclusive for all users.

3. CONCLUSION

Cyberbullying and cyberstalking are growing concerns in India, impacting individuals' mental health, emotional well-being, and overall digital safety. To combat these issues effectively, a holistic and multifaceted approach is necessary. The proposed measures to secure against cyberstalking and cyberbullying in India include robust cyber laws and enforcement, public awareness and education campaigns, reporting mechanisms, and collaboration with tech companies. Additionally, specialized cybercrime units, data protection and privacy measures, counselling and support services, promoting responsible online behavior, fast-track courts, and international collaboration play crucial roles in curbing cyber harassment.

By implementing these measures collectively and involving various stakeholders, the Indian government can foster a safer and more secure digital environment for its citizens. Empowering individuals with knowledge and tools to protect themselves, while holding perpetrators accountable, is essential in creating a digital landscape that encourages respect, empathy, and responsible online conduct. As technology continues to evolve, ongoing efforts, research, and adaptability are essential to stay ahead of cyber threats and create a safer online space for everyone. With the rapid expansion of digital platforms, cyberstalking and cyberbullying have become significant concerns in India. These online threats not only cause psychological distress but also, in some cases, lead to real-world consequences, including self-harm and reputational damage. To effectively safeguard individuals, a multifaceted approach involving legal measures, education,

[7] *Digital Personal Data Protection (DPDP) Act, 2023: This act, effective from 2024, is a significant step towards personal data protection and privacy enforcement in India.*

technological advancements, and community participation is required. Below are some key strategies to combat cyberstalking and cyberbullying in India:

CONFLICT OF INTERESTS

None.

ACKNOWLEDGMENTS

None.

REFERENCES

Indian Penal Code (IPC), 1860. URL: https://indiankanoon.org/doc/553254/
Information Technology (IT) Act, 2000. URL: https://meity.gov.in/content/information-technology-act-2000
Data Protection Laws in India. URL: https://www.meity.gov.in/writereaddata/files/The_Data_Protection_Bill_2019_Data_Privacy.pdf
Cyber Crime Awareness and Prevention Initiatives by Ministry of Home Affairs, India. URL: https://mha.gov.in/sites/default/files/cyber-crime.pdf
National Crime Records Bureau (NCRB) - Cyber Crimes in India (Latest Reports). URL: https://ncrb.gov.in/en/crime-india
UNICEF India - Cyberbullying and Its Impact on Children. URL: https://www.unicef.org/india/what-we-do/child-protection/cyberbullying
Ministry of Electronics and Information Technology (MeitY) - Government of India. URL: https://www.meity.gov.in/
National Cyber Crime Reporting Portal - Ministry of Home Affairs, India. URL: https://cybercrime.gov.in/
National Cyber Security Coordinator - Government of India. URL: https://www.ncsc.gov.in/
National Crime Records Bureau (NCRB) - Reports on Cyber Crimes in India. URL: https://ncrb.gov.in/
UNICEF India - Reports and Initiatives on Cyberbullying and Child Protection. URL: https://www.unicef.org/india/
https://www.comparitech.com/internet-providers/cyberbullying-statistics/
https://blog.securly.com/the-10-types-of-cyberbullying/
ttps://www.statista.com/statistics/1013569/facebook-bullying-and-harassment-content-removal-quarter/
https://en.wikipedia.org/wiki/Akancha_Srivastava_Foundation?utm_source
https://enough.org/stats_cyberb
https://online.maryville.edu/blog/what-is-cyberbullying-an-overview-for-students-parents-and-teachers/
https://www.stopbullying.gov/resources/laws
https://www.findlaw.com/criminal/criminal-charges/cyber-bullying.html
https://www.cybersmile.org/advice-help/category/cyberbullying-and-the-law
https://www.mondaq.com/india/social-media/1193320/cyberstalking-and-the-indian-jurisprudence
https://www.techtarget.com/searchsecurity/definition/cyberstalking
https://www.casemine.com/search/in/course%2Bof%2Bconduct%2Bstalking