Analysis

Cyberbullying on Social Networks – A Crime in India

Aastha Johri[1]*, Dr. Rajiv Singh[2]

ABSTRACT

Cyber bullying on social networks is a serious issue with significant legal and social implications. It involves the use of digital communication tools such as social media platforms, instant messaging, or email to harass, intimidate, or harm others. Cyberbullying can take various forms, including spreading rumors, posting hurtful comments or messages, sharing embarrassing photos or videos, and creating fake profiles or accounts to impersonate or harass someone. From a legal standpoint, cyber bullying may be considered a crime depending on the jurisdiction and the severity of the actions. Laws regarding cyber bullying vary from one place to another, but many countries have enacted legislation to address this problem. For instance, some jurisdictions have specific laws that criminalize cyber bullying behaviors, while others may apply existing harassment, stalking, or defamation laws to prosecute cyber bullies. Social media platforms also play a role in combating cyber bullying by implementing policies and mechanisms to address abusive behavior. They often provide users with tools to report harassment and abuse, and may take action such as suspending or banning accounts that violate their community guidelines. In addition to legal measures and platform policies, raising awareness about the consequences of cyber bullying and promoting digital citizenship and empathy are important steps in preventing and addressing this issue. Educating individuals, especially young people, about responsible online behavior and fostering a culture of respect and kindness can help create safer online environments for everyone.

Social network
Social networks are online platforms that facilitate social interaction and networking among individuals or groups of people. These platforms allow users to create personal profiles, share content such as photos, videos, and text-based posts, and connect with others who share similar interests or backgrounds. Some of the most popular social networks include Facebook, Twitter, Instagram, LinkedIn, Snapchat, and TikTok.

Social networks serve various purposes, including:

- **Connecting with Friends and Family:** Social networks provide a convenient way for people to stay in touch with friends and family members, regardless of

---

[1]Research Scholar

[2]Department of Computer Science, Faculty of Mathematics and Computing Banasthali Vidhyapeeth, Newai
*Corresponding Author

geographical distance. Users can share updates about their lives, photos, and videos, and engage in conversations in real-time.

- **Networking:** Social networks are valuable tools for professional networking. Platforms like LinkedIn are specifically designed for connecting with colleagues, mentors, and potential employers, as well as for sharing professional achievements and industry insights.
- **Sharing Content:** Social networks allow users to share various types of content, including photos, videos, articles, and status updates. This content can be shared publicly or with a select group of friends or followers, depending on the user's privacy settings.
- **Discovering New Interests and Trends:** Social networks often feature algorithms that curate content based on users' interests and behavior. This can expose users to new ideas, trends, and communities that they might not have encountered otherwise.
- **Promoting Businesses and Brands:** Businesses and brands use social networks as marketing platforms to reach and engage with their target audiences. Social media marketing strategies may involve creating branded content, running targeted advertisements, and interacting with customers and followers.
- **Facilitating Social Activism and Awareness:** Social networks have been instrumental in raising awareness about social and political issues, organizing grassroots movements, and mobilizing support for various causes. Platforms like Twitter and Instagram are often used to amplify voices and share information about important social issues.

While social networks offer many benefits, they also pose certain risks, including privacy concerns, cyberbullying, misinformation, and addiction. It's important for users to be mindful of how they use social media and to take steps to protect their privacy and well-being while engaging with these platforms.

cyberstalking is indeed considered a crime in many jurisdictions. Cyberstalking involves the use of electronic communications to repeatedly harass or threaten someone, causing them fear or emotional distress. This behavior can take various forms, including sending threatening emails, messages, or social media posts, monitoring someone's online activity without their consent, or using technology to track someone's movements. Laws regarding cyberstalking vary by country and state, but many jurisdictions have specific statutes in place to address this type of harassment and protect victims.

LAWS FOR CYBERTALKING IN INDIA

In India, cyberstalking and related offenses are addressed under the Information Technology (IT) Act, 2000, and its subsequent amendments. The relevant sections of the IT Act that deal with cyberstalking include:

- **Section 66A:** This section, which was struck down by the Supreme Court of India in 2015 for being unconstitutional, previously dealt with "sending offensive messages through communication service."
- **Section 67:** This section deals with the publishing or transmitting obscene material in electronic form, which can include sexually explicit messages sent for the purpose of harassment.
- **Section 67A:** This section deals with publishing or transmitting sexually explicit material in electronic form, which can also be used to prosecute cyberstalking involving sexually explicit content.

- **Section 67B:** This section deals with the punishment for publishing or transmitting material depicting children in sexually explicit acts, which can apply to cases of cyberstalking involving child exploitation.
- **Section 72:** This section deals with the breach of confidentiality and privacy, which could be relevant in cases where private information is obtained and used for stalking purposes.

Additionally, the Indian Penal Code (IPC) contains provisions that can be used to prosecute cyberstalking, such as:

- **Section 354D:** This section deals with stalking, whether physical or through electronic communication, and provides for punishment for the same.
- **Section 509:** This section deals with word, gesture, or act intended to insult the modesty of a woman, which can include online harassment and stalking.

HOW INDIA CAN MINIMIZE THE CRIME OF CYBERTALKING

Minimizing cyberstalking in India requires a multifaceted approach involving legal, technological, educational, and societal measures. Here are some strategies that can help:

- **Strengthening Legal Frameworks:** Continuously update and strengthen laws related to cybercrimes, including cyberstalking, to ensure they are comprehensive and effective in addressing evolving forms of online harassment. This may involve introducing new legislation, amending existing laws, and providing clear definitions and penalties for cyberstalking offenses.
- **Law Enforcement Training:** Provide specialized training to law enforcement agencies to effectively investigate and prosecute cyberstalking cases. This includes training on digital forensics, cybercrime investigation techniques, and understanding the psychological impact of cyberstalking on victims.
- **Awareness and Education:** Increase public awareness about cyberstalking and its consequences through campaigns, workshops, and educational programs. This includes educating individuals about online safety, privacy settings, and the importance of reporting cyberstalking incidents to the authorities.
- **Victim Support Services:** Establish support services for cyberstalking victims, including helplines, counseling, and legal assistance. Ensure that victims feel safe and supported when reporting cyberstalking incidents and seeking help.
- **Technological Solutions:** Develop and implement technological solutions to prevent and combat cyberstalking, such as improved cybersecurity measures, anti-stalking software, and tools for detecting and blocking malicious online behavior.
- **International Cooperation:** Foster cooperation and collaboration with international law enforcement agencies and organizations to address cross-border cyberstalking cases effectively. This includes sharing information, resources, and best practices for combating cybercrimes on a global scale.
- **Community Engagement:** Encourage active involvement from communities, schools, and other institutions in preventing cyberstalking and promoting online safety. This can involve organizing awareness events, creating safe online spaces, and fostering a culture of respect and empathy among internet users.
- **Research and Data Collection:** Invest in research and data collection efforts to better understand the prevalence, patterns, and impact of cyberstalking in India. This information can inform policy decisions, resource allocation, and prevention strategies aimed at reducing cyberstalking incidents.

Future of Cybertalking

The future of cyberstalking is shaped by advancements in technology, evolving social norms, and changes in legal frameworks. Here are several key trends and potential developments:

1. Technological Advancements

- **Artificial Intelligence (AI) and Machine Learning:** AI can be used both for and against cyberstalking. While AI-driven tools can help stalkers gather and analyze personal information more efficiently, the same technologies can also enhance detection and prevention measures.
- **Enhanced Surveillance Capabilities:** Improvements in digital surveillance tools, including facial recognition, GPS tracking, and data mining, could make it easier for stalkers to monitor and harass their victims.
- **Internet of Things (IoT):** The proliferation of IoT devices increases the number of entry points for cyberstalkers. Smart home devices, wearables, and connected cars can all be exploited to track and harass individuals.

2. Evolving Social Media Platforms

- **Anonymity and Pseudonymity:** Social media platforms may continue to struggle with balancing user privacy and security. Features that protect user anonymity can be misused by cyberstalkers.
- **Augmented Reality (AR) and Virtual Reality (VR):** As AR and VR become more mainstream, they could create new venues for cyberstalking. These immersive environments might be exploited to harass individuals in more personal and invasive ways.

3. Legal and Regulatory Changes

- **Stricter Legislation:** Governments are likely to enact stricter laws to address cyberstalking, driven by increasing awareness and public demand for safety.
- **International Cooperation:** As cyberstalking often crosses national borders, international cooperation and agreements will be essential to effectively combat it.

4. Enhanced Cybersecurity Measures

- **Advanced Detection Tools:** The development of sophisticated algorithms and machine learning models can help detect and prevent cyberstalking activities more effectively.
- **User Education and Awareness:** Increased awareness and education on cyberstalking can empower users to protect themselves. Cybersecurity literacy programs could become more widespread and integrated into educational curricula.

5. Psychological and Social Impacts

- **Increased Mental Health Support:** The psychological toll of cyberstalking is significant. Future trends might see an increase in mental health resources and support for victims.
- **Social Stigma and Awareness:** Greater societal awareness and reduced stigma associated with being a victim of cyberstalking can encourage more individuals to seek help and report incidents.

6. Corporate Responsibility

- Platform Accountability: Social media and tech companies might be held more accountable for cyberstalking incidents that occur on their platforms. This could lead to stricter content moderation policies and proactive measures to prevent harassment.

CONCLUSION

The future of cyberstalking will be influenced by a combination of technological, legal, social, and psychological factors. While advancements in technology provide new tools for stalkers, they also offer innovative solutions for detection and prevention. Legal reforms and increased awareness can help create a safer online environment. However, it will require continuous efforts from individuals, tech companies, and governments to effectively combat cyberstalking.

By implementing these strategies in a coordinated manner, India can work towards minimizing the crime of cyberstalking and creating a safer and more secure online environment for its citizens. These laws collectively provide a legal framework to address cyberstalking and related offenses in India. However, it's essential to consult legal professionals for the most accurate and up-to-date information regarding cyber laws in the country.

REFERENCES

Slonje R, Smith PK, Frisén A. Processes of cyberbullying, and feelings of remorse by bullies: A pilot study. *Eur J Dev Psychol.* 2012; 9: 244–59.

Cassidy W, Jackson M, Brown KN. Sticks and stones can break my bones, but how can pixels hurt me?: Students' experiences with cyber-bullying. *Sch Psychol Int.* 2009; 30: 383–402.

S. Agrawal and A. Awekar, "Deep learning for detecting cyberbullying across multiple social media platforms", *In European Conference on Information Retrieval*, pp. 141-153, 2018.

M. Dadvar and K. Eckert, "Cyberbullying Detection in Social Networks Using Deep Learning Based Models; A Reproducibility Study", *arXiv preprint arXiv:1812.08046* , 2018.

L. Cheng, J. Li, Y. N. Silva, D. L. Hall and H. Liu, "XBully: Cyberbullying Detection within a Multi-Modal Context", *In Proceedings of Twelfth ACM International Conference on Web Search and Data Mining*, pp. 339-347, 2019.

Niharika Thakkar, Mitch van Geel and Paul Vedder, "A Systematic Review of Bullying and Victimization Among Adolescents in India", *2020 Springer International Journal of Bullying Prevention*.

Manuel F. López-Vizcaíno, Francisco J. Nóvoa, Victor Carneiro and Fidel Cacheda, "Early detection of cyberbullying on social media networks", *Elsevier 2021 Future Generation Computer Systems*, vol. 118, pp. 229, 2021.