ISSN (O): 2584-2196

INTERNATIONAL JOURNAL OF LEGAL AFFAIRS AND EXPLORATION

Volume 3 | Issue 2

2025

Website: www.ijlae.com

Email: editor@ijlae.com

ISSN (O): 2584-2196

THE ROLE OF SOCIAL MEDIA IN SHAPING ADMINISTRATION OF JUSTICE: A CRITICAL ANALYSIS OF CYBERCRIME AND ONLINE HARASSMENT

Chunduru Deepthi

LL.M. Student, REVA University, Bengaluru

ABSTRACT

The advent of social media has changed the way individuals engage with each other, and it has provided a platform for interaction, sharing, and information dissemination. The revolution came with greater challenges to the administration of justice, particularly on issues of cybercrime and harassment on the internet. Social media, in enabling the users, has also proven to be fertile ground for every type of cybercrime such as hacking, identity theft, cyberbullying, and internet harassment. This essay critically examines the contribution of social media to the administration of justice, and the nexus between social media and cybercrime and internet harassment. The essay examines the dominant legal frameworks in India and globally, including loopholes and obstacles to the prosecution of cybercrimes. Additionally, the essay examines the ethical and pragmatic issues faced in regulating offending content on social media without infringing freedom of expression and privacy rights. It ends on the note of suggestions to enhance legal action and enhance coordination between social media and law enforcement agencies to combat cybercrime more effectively.

Keywords: *- Cyberbullying, Legal systems, Information Technology Act, social media, Online intimidation, Cybercrime, Police, Right to privacy, Freedom of speech, Justice digital.*

INTRODUCTION

Social media has largely re-shaped the manner in which human beings communicate, socialize, and interact with each other in today's global online community. Due to Facebook, Twitter, Instagram, and WhatsApp's increased presence in our lives, they have contributed so much to society, such as social life,

ISSN (O): 2584-2196

public life, politics, and lawmaking. Though these sites have made communication and interaction easier, they have also brought an array of legal problems at their core the subject of cyberbullying and cybercrime. The anonymity of internet social sites and the global nature of the web have created an environment in which harassing behavior—anything from cyberbullying to cyberstalking and cyber libel—can be done easily, with far too little rapid accountability. The growing number of such challenges has raised questions regarding how the legal system can adapt to meet these new challenges. Justice administration, which previously was founded on territorial and geographical boundaries, now has the challenge of governing conduct in a space that is beyond national jurisdiction. This shift has challenged traditional legal regimes and the need to reimagine justice administration in the cyberspace. In India, the Information Technology Act 2000 and its amendments have been the main legislations fighting cybercrimes. But the increasing sophistication of cybercrime and the rapid development of social media have exposed the limitations of such a law in addressing modern online crime. The spread of online harassment, particularly, has been a huge threat to the safety and well-being of individuals, particularly women and marginalized communities, in the virtual world. This paper attempts to critically analyze the contribution of social media in the administration of justice, with emphasis on cybercrime and cyber-harassment. In a review of the existing models of law, the paper attempts to analyze their adequacy in addressing the new challenges. The paper also addresses the issue of dispense of justice online, with emphasis on the disciplines of ethics on privacy, freedom of speech, and censorship of the internet. Finally, the article also attempts again to underscore the urgent necessity of far-reaching legal reforms to protect the people from the mounting menace of cyberbullying and cybercrime in the current age of cyberspace.

THE ROLE OF SOCIAL MEDIA IN MODERN SOCIETY

Social networking sites have revolutionized how humans interact and socialize with each other. Websites like Facebook, Twitter, Instagram, and WhatsApp have become so much a part of daily lives that people just cannot live without them, bringing instant communication, collaboration, and information sharing between people. From billions of fans across the world, social networks have transformed human consumption of news, political exchange, and even relationships. They have transformed into online platforms where individuals share personal stories, professional success stories, and observations on everything from productivity tips to events in the world and life events.[1] The arrival of social media has

[1] Shankar, "Social Media and Its Impact on Communication," Journal of Digital Media Studies (2021) 45(3): 58.

ISSN (O): 2584-2196

resulted in profound repercussions for most sectors, such as politics, enterprise, entertainment, and law. Social media has given people power to express themselves, mobilize for causes, and engage with the public as never before. Political movements, including the Arab Spring and the MeToo movement, demonstrate how social media use the tools to challenge power, raise awareness of seriously serious causes, and advance social change. Social media platforms, through virality and hashtags, have been successful as tools for campaigning and activism.[2] But social media's impact does not stop at the positive on society. Social media has also brought new issues, like the regulation of dangerous content and activity. Social media anonymity provides users with ease of access to and participation in things they would not do offline. This has allowed a host of different cybercrime and cyberbullying to be performed, and individuals to have been so courageous as to utilize cyberspace with no immediate reaction. The site also accentuates the spreading of disinformation, hate messages, and slanderous content, with colossal societal and legal consequences. As social media continues to be at society's core, issues like this are becoming increasingly scrutinized with regard to legality and morality. In order to address all of these issues, governments and agencies across the globe have started establishing laws and regulations to prevent harmful activities on social media. For instance, the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, in India were enacted with the objective of handling cyber bullying, harassment, and data breach cases. On top of this, the new guidelines for intermediaries, brought out by the Ministry of Electronics and Information Technology (MeitY) in 2021, also put social media platforms into greater onus to monitor and police user-created content. However, how useful the regulations end up being, only time will tell, with jurisdictions such as issues with jurisdiction and freedom of speech taking a backseat over policing harmful content.[3] Whereas social media has ushered in vast social transformation and change, it has equally introduced an abundance of new legal intricacies. The question then is how to ensure continued access to social media as a forum for free expression while protecting individuals from bad behavior. The legal regimes currently established need to be able to keep up with the rapidly evolving mechanisms of digital communication to enable justice to be made accessible to everyone using social media

[2] Ghosh, "Political Activism in the Age of Social Media: A Study of the Arab Spring," International Journal of Political Science (2020) 12(1): 23-24.

[3] Ministry of Electronics and Information Technology, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Notification No. 1(2)/2011-Cyber Law.

ISSN (O): 2584-2196

UNDERSTANDING CYBERCRIME AND ONLINE HARASSMENT

Cybercrime can be defined as criminal activity conducted via computers, networks, or the internet. Cyber platforms have been established, and different types of cybercrime have emerged from identity theft and financial fraud to cyberbullying and online harassment. In contrast to crimes in physical locations, cybercrimes are conducted in cyberspace, frequently across borders, and thus jurisdictional enforcement becomes challenging. The character of the anonymity of the net provides a feeling of impunity to the criminal, which makes it harder to pursue such crimes successfully. Cybercrime is a fairly vague term for activity, but they can be roughly categorized into two very vague groups: crimes against individuals and crimes against governments or organizations. Crimes against individuals are things like identity theft, cyberbullying, and harassment on the internet. They do emotional, psychological, and financial harm to their victims. Crimes against a government or an organization are likely to be cyber theft, hacking, cyber espionage, or cyberterrorism. Since they are cybercrimes, the culprits can commit them anywhere on the face of the earth, and it is hard for the local law enforcement officers to trace them and bring them to book.[4]Harassment and cyberbullying are the most prevalent forms of cybercrime affecting individuals directly. Cyberbullying refers to a form of harassment, threat, or intimidation via the internet by employing a person's personal data and information. Cyberbullying takes many forms like sending threatening e-mails, defamation of social media via social networking websites, or propagation of false rumors via the internet. The consequences of cyberbullying are devastating, and they may cause emotional distress, depression, and in severe cases, self-mutilation, or suicide. The victims of cyberbullying tend to feel powerless since the abuse might be occurring 24/7 and even find its way offline. Harassment on the internet, although akin to cyberbullying, is broader in scope and need not include minors or a particular social group. It includes any offensive, threatening, or unwanted conduct against a person using the internet. Doxxing (public disclosure of identifying information), stalking, and sending unsolicited explicit content are examples. Both online bullying and cyber harassment are most common on social networking platforms since the simplicity of opening anonymous accounts and getting a big following increases the potential for damage.[5] Legal framework to prevent cybercrime and cyber harassment is varying in every jurisdiction, but the Information Technology Act of 2000[6] and the amendments have been the pivotal law to regulate cybercrimes in India. Section 66A of the Act, which

[4] Sharma, "Understanding the Dynamics of Cybercrime in India," Journal of Cybersecurity Law (2021) 16(2): 44-46.
[5] Gupta, "The Legal Framework for Cyberbullying in India: A Critical Review," Indian Journal of Technology and Law (2020) 31(4): 99.
[6] The Information Technology Act, 2000, Section 66A, Government of India, Ministry of Electronics, and Information Technology.

criminalized sending offensive messages through the services of a computer resource, was struck down as unconstitutional by the Supreme Court in 2015, and there was a call for tougher and focused legislation on cybercrimes and cyber harassment. However, Indian Penal Code (IPC) provisions such as Section 354C (Voyeurism) and Section 509 (Word, gesture, or act intended to insult the modesty of a woman) continue to be employed for cyber stalking and cyber harassment over the internet.[7] Despite such laws, criminal prosecution of cybercrimes remains an issue. The jurisdictional problem is complex, with the crime usually being committed from outside the country, where it cannot be prosecuted under local law. Victims also are unaware of what legal action can be taken against them or are reluctant to complain because they are afraid their privacy will be breached or victimized by retaliation.[8] International coordination and leadership by tech companies are required in meeting these challenges. Although most social networking websites have implemented reporting by users to pinpoint offending content, efforts have been seen across the board as insufficient. Additionally, websites have been faulted for being slow to remove abusive postings or sanction people for doing so. There has also been a call recently for social sites to be regulated, with governments calling for greater control over the sites to have them accountable for the content that they have hosted.

SOCIAL MEDIA AS A TOOL FOR CYBERCRIME AND HARASSMENT

Social media websites have revolutionized communication in that individuals can discuss, share information, and state opinions. Social media websites have also been hijacked by offenders in a bid to carry out all forms of criminal activities. The cybercrimes have also mastered ways of living in the online world availed by social media, using it to conduct their illicit activities, including stealing identities, fraudulent activities, stalking, and intimidation. The anonymity and the sheer scale of social media provide the ideal setting for these crimes to be committed.[9] The most common social media cybercrime is identity theft. Social media websites where individuals have posted personal information are used by cybercriminals to gain access to private personal information which they utilize to carry out scams, for instance, opening a bank account or receiving credit cards issued in an individual's name. Since the majority of people post their date of birth, residential address, along with their fiscal details online voluntarily, cyber criminals misuse the data to steal identities.[10] But, yet another very popular type of

[7] · Mehta, "Online Harassment and Legal Solutions: The Indian Context," Journal of International Cyber Law (2022) 18(1): 17.
[8] Chawla, "The Role of Social Media Platforms in Combating Cybercrime," Digital Law Review (2022) 27(3): 62.
[9] P. Srivastava, “Understanding Identity Theft in the Age of Social Media,” Cyber Law Review (2021) 27(3): 64.
[10] D. Sharma, “Privacy Concerns in Social Media: A Legal Perspective,” Indian Bar Journal (2020) 46(1): 22.

ISSN (O): 2584-2196

social media cybercrime is disinformation and scams. From copying fundraising campaigns to phishing, social media websites have become playgrounds for spammers who want to deceive individuals. Scammers can impersonate genuine companies, banks, or even friends and relatives to trick people and manipulate them into providing information about themselves or sending money. These are typically in the form of sincere offers or pathetic pleas, banking on the credulity and trustworthiness of social media users. Harassment and cyber bullying also occur on social networking websites, where individuals use the same websites to harass others using abusive behavior. This may include the posting of abusive rumors, abusive comments, or abusive messages. Social media's provision of allowing individuals to be anonymous is likely to lead to the commission of these acts of abuse. In most cases, cyberbullying and harassment victims endure severely from emotional as well as psychological harm, and their consequences are felt for a long time, such as depression and anxiety. Social media culture of 24/7 also ensures that harassment continues without pause, piling the victim with misery[11]. In addition to that, revenge pornography or non-consensual sharing of nude photographs is another serious type of cyber harassment that has been brought about by the spread of social media. Criminals would typically publish nude photographs or videos of a person, commonly an ex-partner, as a means of embarrassing or intimidating them. This type of harassment is not only psychologically harmful but also an invasion of an individual's right to privacy and dignity, which has legal and societal implications. The challenge of fighting cybercrime and social media bullying is also compounded by the global web. It is easy for cybercriminals to operate from countries where the law does not much care, making it a jurisdictional nightmare for law enforcers. Moreover, technology is advancing at such a rate that criminals never cease to discover new means of exploiting social media vulnerabilities.[12]

THE ROLE OF SOCIAL MEDIA IN SHAPING THE LEGAL RESPONSE TO CYBERCRIME

The rising trend of cybercrime and cyber harassment on social media has led to the re-evaluation of legal frameworks. As most cases are cybercrimes, parliament has tried to reform and improve existing laws, though the process has not been smooth. In India, the Bhartiya Nyaya Sanhita, 2023 (BNS) [13]has introduced new provisions to address cybercrimes, including cybercrimes centered on social media. New special cyberstalking, defamation, and identity theft categories have been introduced to address criminal

[11] M. Tripathi, "Online Abuse and Platform Accountability," Indian Journal of Cyber Law (2023) 12(1): 93.
[12] S. Gupta, "Transnational Cybercrime: Challenges to Indian Law Enforcement," Criminal Law Review (2020) 50(1): 30.
[13] Bhartiya Nyaya Sanhita, 2023, Section 230, Government of India.

ISSN (O): 2584-2196

abuse of social media. Under the BNS, internet harassment can be penalized by whoever does something that brings disrepute to a person's dignity, privacy, and reputation, whether digitally or otherwise. Though the BNS has progressed a long way in passing anti-cybercrime laws, their enforcement is still a cause of concern. The social networking websites are utilized transborder-wise, and it is challenging to identify and prosecute the users of the same for criminal intentions. This again poses serious issues of jurisdiction and extraterritoriality of domestic law. Along with the BNS, the Government of India's Intermediary Guidelines and Digital Media Ethics Code, 2021, requires more content moderation policy and greater accountability on the part of social media platforms for the user-uploaded content. The companies are now required to appoint compliance officers and have a grievance redressal mechanism for the users. The guidelines safeguard users and hold the platforms responsible for illegal activities taking place on the platforms. Despite all these efforts, cybercrime and social media harassment regulation is still plagued by many challenges. Perhaps the greatest challenge is how policymakers balance freedom of speech and safeguarding individuals from harmful content. Social media platforms must balance individuals being shielded from harassment with users' freedom of expression as well. Balancing in this case is a fine line for policymakers and regulators to walk.[14]Apart from this, social networks themselves have been proactive in initiating legal action against cybercrime. Facebook, Twitter, and Instagram are some of the networks that have implemented procedures for complaining about objectionable material, including insulting posts, threats, or abusive posts. The procedures are, however, deficient in so far as they are slow or ineffective in removing nasty material even if it remains available on the net although intended to be deleted. A number of websites have utilized AI technology to automatically delete and detect offending material, but AI technology is imperfect. Furthermore, users alleged that websites censor legitimate speech or discriminate in censoring material, raising controversy regarding the limits of control of speech across the Internet. Regardless of such challenges, the role of social media in legal reactions to cybercrime cannot be undone. With increasing takeover by social media, social media sites and laws that regulate them will also have to evolve to effectively counter dangers from crimes committed through the internet and online bullying effectively.[15]

ETHICAL AND PRACTICAL CHALLENGES IN ENFORCING JUSTICE

[14] S. Gupta, "Transnational Cybercrime: Challenges to Indian Law Enforcement," Criminal Law Review (2020) 50(1): 30.
[15] Ministry of Electronics and Information Technology, IT Rules 2021, Gazette Notification, Part II, Section 3(ii), 25 February 2021.

ISSN (O): 2584-2196

Regardless of the amendments such as the Bhartiya Nyaya Sanhita (BNS), 2023, and the Intermediary Guidelines, 2021, for making the law more effective against cybercrime and cyberbullying, the administration of justice in cyberspace is marred with dubious ethical and practical issues. Apparently, the strongest ethical issue is a balance between freedom of expression and the removal of offending content. Overregulation or under regulation of content can result in censorship of minorities, satire, or dissenting opinion. Article 19(1)(a) of the Indian Constitution imposes the constitutional freedom of expression under reasonable restrictions but leaves gateways to obscurity while defining "reasonable" in interpreting online speech in making it frustrating for law enforcement bodies and social networking websites as well.[16] Also, there are moral considerations at stake with AI content moderation. The automated moderation system might not be able to sense context, irony, or linguistic nuance and thus create false positives where legal speech is moderated out, or false negatives where offending material is not caught.[17] In addition to infringing on the right to expression, this also undermines the public's trust in digital government processes. In practice, the global and anonymous nature of the internet prevents prying and investigation. Criminals can use the veil of virtual private networks (VPNs), proxy servers, or dark web channels and cannot be traced by the authorities.[18] Moreover, when such a crime has international borders, jurisdictional conflicts occur, especially if the host country has poor cyber law or recalcitrant legal systems. There even lacks cyber forensic capability in the police force in India. There is no highly sophisticated equipment, nor trained officials, in the majority of police forces to appropriately investigate cybercrime. This usually results in delaying or failing to prosecute cyber criminals, thereby rendering the benign intention of provisions of the Bhartiya Nyaya Sanhita. Its lack is also an ethical shortcoming. The majority of the victims of online harassment—especially women and sexual minorities—are exposed to social exclusion, blaming the victim, and institutional negligence.[19] The inability of the legal system to impart timely protection and psychological rehabilitation to the victims discouraging reporting and eroding common faith in judicial redress.

CONCLUSION

[16] Constitution of India, Article 19(1)(a), read with Article 19(2), Government of India.
[17] Bansal S, "AI Bias in Moderation Systems: Legal and Ethical Ramifications" (2022) 14(2) Indian Journal of Tech Law 98.
[18] Sharma A, "Jurisdictional Challenges in Cybercrime Enforcement" (2021) 18 Criminal Law Review 127.
[19] Ministry of Home Affairs, "Cyber Crime Investigation Capacities in Indian Police Forces," Government Report, 2022.

ISSN (O): 2584-2196

Social media is also proving to be a deeply powerful force that, on the one hand, is enabling democratic engagement and, on the other, giving rise to novel forms of criminality. As critically debated in this article, cybercrime and cyberbullying are becoming issues that call for brilliant, smart legal responses. India's efforts in the Bhartiya Nyaya Sanhita, 2023, and Intermediary Guidelines, 2021, are an encouraging move, but enforcement continues to be stymied by moral concerns, technology challenges, and jurisdictional problems. To make administration of justice in the age of the internet effective and fair, legal reform must be balanced with ethical protection, international cooperation must be increased, digital capacity and police capability built up. Meanwhile, the active participation of social media companies in content moderation and supporting victims cannot be exaggerated. Ultimately, the development of a more secure virtual society is a product of concerted actions on the part of the state, online venues, civil society, and society as a whole. Only by cooperation can justice effectively be delivered within a rapidly changing cyber community.

ISSN (O): 2584-2196

REFERENCES

1. *Shankar, "Social Media and Its Impact on Communication," Journal of Digital Media Studies (2021) 45(3): 58.*
2. *Ghosh, "Political Activism in the Age of Social Media: A Study of the Arab Spring," International Journal of Political Science (2020) 12(1): 23-24.*
3. *Ministry of Home Affairs, "Cyber Crime Investigation Capacities in Indian Police Forces," Government Report, 2022.*
4. *Ministry of Electronics and Information Technology, IT Rules 2021, Gazette Notification, Part II, Section 3(ii), 25 February 2021.*
5. *Constitution of India, Article 19(1)(a), read with Article 19(2), Government of India.*
6. *Bansal S, "AI Bias in Moderation Systems: Legal and Ethical Ramifications" (2022) 14(2) Indian Journal of Tech Law 98.*
7. *Sharma A, "Jurisdictional Challenges in Cybercrime Enforcement" (2021) 18 Criminal Law Review 127.*
8. *S. Gupta, "Transnational Cybercrime: Challenges to Indian Law Enforcement," Criminal Law Review (2020) 50(1): 30.*
9. *[1] Bhartiya Nyaya Sanhita, 2023, Section 230, Government of India.*
10. *[1] S. Gupta, "Transnational Cybercrime: Challenges to Indian Law Enforcement," Criminal Law Review (2020) 50(1): 30.*
11. *P. Srivastava, "Understanding Identity Theft in the Age of Social Media," Cyber Law Review (2021) 27(3): 64.*
12. *[1] D. Sharma, "Privacy Concerns in Social Media: A Legal Perspective," Indian Bar Journal (2020) 46(1): 22.*
13. *[1] M. Tripathi, "Online Abuse and Platform Accountability," Indian Journal of Cyber Law (2023) 12(1): 93.*
14. *[1] S. Gupta, "Transnational Cybercrime: Challenges to Indian Law Enforcement," Criminal Law Review (2020) 50(1): 30.*
15. *[1] Bhartiya Nyaya Sanhita, 2023, Section 230, Government of India.*
16. *[1] S. Gupta, "Transnational Cybercrime: Challenges to Indian Law Enforcement," Criminal Law Review (2020) 50(1): 30.*

ISSN (O): 2584-2196

17. *Ministry of Electronics and Information Technology, Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, Notification No. 1(2)/2011-Cyber Law.*

18. *Sharma, "Understanding the Dynamics of Cybercrime in India," Journal of Cybersecurity Law (2021) 16(2): 44-46.*

19. *[1] Gupta, "The Legal Framework for Cyberbullying in India: A Critical Review," Indian Journal of Technology and Law (2020) 31(4): 99.*

20. *[1] The Information Technology Act, 2000, Section 66A, Government of India, Ministry of Electronics, and Information Technology.*

21. *[1] · Mehta, "Online Harassment and Legal Solutions: The Indian Context," Journal of International Cyber Law (2022) 18(1): 17.*

22. *[1] Chawla, "The Role of Social Media Platforms in Combating Cybercrime," Digital Law Review (2022) 27(3): 62.*