f Law

o*International Journal of Law, Justice & Statutory Affairs*
Volume 1, Issue 2, 2025

Social media and cybercrime: Legal responsibility in the Indian setting

Kabiru Garba Muhammad
Department of Law
Himachal Pradesh University, Summerhill, Shimla, Himachal Pradesh, India

Research Article

Date of Submission: 12-04-2025 **Date of Acceptance: 29-05-2025** **Date of Publication: 16-06-2025**

Abstract
India's legal system faces significant issues as a result of the social media platforms' explosive expansion, which has changed communication, business, and government while also increasing the possibility of cybercrime. This research looks at the many aspects of cybercrime on social media, including financial fraud, online harassment, identity theft, disinformation, hate speech, and child exploitation. It examines judicial views of intermediary responsibility, free expression, privacy, and public order as well as the regulatory environment under the Information Technology Act of 2000. The report emphasises how technology both facilitates and lessens cybercrimes and suggests that stakeholders work together to improve accountability while defending constitutional rights. The goal of this thorough research is to add to the current discussion about striking a balance between innovation and regulation in the digital sphere.

Keywords: Social media, cybercrime, Indian law, judicial interpretation, intermediary responsibility, privacy, and free expression

Introduction

Social media platforms have become essential instruments for engagement, commerce, and government in the digital age, which has completely changed communication. These platforms promote connectedness, but they also act as havens for cybercrimes including hate speech, identity theft, online abuse, and disinformation. The judicial system in India, where social media is widely used, must both protect digital liberties and uphold responsibility. Although cyber activities are intended to be regulated under the Information Technology Act of 2000 and its later revisions, the increase in cybercrime events reveals serious inadequacies [1]. This paper looks at the legislative framework that governs cybercrime, assesses the obligations of social media intermediaries, and suggests ways to improve accountability in the Indian environment while striking a balance between user rights and privacy.

The Nature of Cybercrime on Social Media Platforms

A variety of cybercrimes are often committed via social media platforms:

1. Online Harassment

Cyberbullying, trolling, cyberstalking, and defamation are all considered forms of online harassment. The anonymity offered by social media sites exacerbates the psychological pain that these crimes often cause to their victims.

Cyberbullying: sending threatening or abusive texts to anyone, often kids. Severe mental discomfort and, in some situations, self-harm may result from this.

- **Cyberstalking:** Persistent and invasive internet behaviour with the intention of threatening or monitoring someone. Stalking, including cyberstalking, is illegal in India under Section 78 of the BNS, 2023.
- **Trolling:** coordinated efforts, sometimes with sexist, casteist, or communal overtones, to offend, degrade, or denigrate people or groups [2].
- **Defamation:** Disseminating false information or defamatory remarks to the public might result in a loss of livelihood and reputation.

f Law

2. Identity Theft

Identity theft is the unlawful exploitation of a person's personal data for fraud or other illicit purposes. Because users exchange so much personal information, social media sites are especially vulnerable to this crime.

Phishing: To trick people into disclosing private information like passwords or bank account information, criminals fabricate profiles or links.

Impersonation: Fraudsters impersonate people via fictitious accounts, which may result in financial fraud or reputational damage. Due to the absence of strong processes on platforms, victims often find it difficult to report and address these situations [3].

3. Misinformation and Fake News

One of the biggest problems with social media is misinformation and false news. Among them are:

Spread of Rumors: Social media creates a fertile ground for rumours that might disturb public order during elections or public crises.

- **Health-Related Misinformation:** As seen during the COVID-19 pandemic, false statements about medical treatments or vaccinations have generated widespread anxiety and reluctance.
- **Political Propaganda:**Intentional initiatives aimed at influencing public opinion or propagating polarising stories. Stricter regulations are required since platforms' algorithms, which are intended to promote interesting material, often magnify false information.

4. Hate Speech and Radicalization

In India's complex and delicate sociopolitical context, hate speech and radicalisation are serious issues. Social media makes it possible to:

Dissemination of Hate Speech: Widespread dissemination of messages that target populations based on gender, caste, or religion often results in violence in the real world.

- **Radicalization and Recruitment:**Extremist organisations use social media's worldwide reach and anonymity to find and enlist susceptible people.
- **Incitement to Violence:** Numerous events employing WhatsApp forwards have shown that viral information may incite riots or mob violence [4].

In the 2021 case of Amitabh Thakur v. Union of India [5], the court emphasised how hate speech spreads on social media and how it affects public order. It instructed platforms to take aggressive steps to moderate material. In these situations, judicial opinions emphasise striking a balance between the right to free speech and the avoidance of injury.

5. Financial Fraud

The following are examples of financial fraud on social media:

Online Scams: 1.Fake ads, Ponzi schemes, or fake freebies targeting naive consumers.

1.

Cryptocurrency Fraud: 2. Unregulated digital currency scams, which are often advertized via deceptive social media postings [6].

6. Child Exploitation and Obscenity

Crimes involving child exploitation and the spread of pornographic material have also been committed on social media platforms. This comprises:

Grooming: Social media is a tool used by predators to take advantage of youngsters by winning their confidence and persuading them into engaging in illicit activities.

- **Dissemination of Explicit Material:** Despite technical developments, platforms find it difficult to identify and stop the distribution of child pornography or other offensive information [7].

In re Prajwala Letter (2018) [8], the Supreme Court ordered social media companies to use cutting-edge technology for identifying and eliminating child pornography.

The courts has pushed for more stringent oversight while upholding consumers' right to privacy.

The Role of Technology in Amplifying Cybercrime

Technological developments have made social media cybercrimes more complex and difficult to stop:

Artificial Intelligence and Deepfakes: AI-generated material, like deepfake movies, may be used to propagate misleading information or as a form of blackmail.

f Law

Encryption and Anonymity: Although encryption protects user privacy, it also makes it possible for criminals to operate covertly [9].

- **Bots and Automated Accounts:** Hate speech and other harmful material are amplified by automated algorithms on a never-before-seen scale.

Legal Framework Governing Cybercrime in India
Information Technology Act, 2000 (IT Act)

The primary law in India that deals with cybercrimes is the IT Act. Hacking and other cybercrimes are defined and punished under Section 66. The transmission of pornographic material is covered under Section 67, which has severe penalties for infractions [10]. Even though Shreya Singhal v. Union of India overturned Section 66A, which made obscene internet postings illegal, the argument between regulation and freedom of expression persists [1].

Intermediary Guidelines and Digital Media Ethics Code Rules, 2021

In order to improve intermediary responsibility, certain regulations were implemented under Section 79 of the IT Act. They require: Grievance officers are appointed to address consumer concerns. Unlawful information must be removed within 36 hours following a court order or government decision. Using automated techniques to proactively detect and eliminate unwanted information [11].

Penal Provisions under Bhartiya Nyaya Sanhita, 2023 (BNS)

The Bhartiya Nyaya Sanhita, 2023 (BNS) and the Indian Penal Code (IPC) both address a number of crimes that are increasingly being perpetrated via social media. Crimes including defamation (Section 499 IPC/Section 356 BNS), criminal intimidation (Section 503 IPC/Section 351 BNS), and inciting animosity between groups (Section 153A IPC/Section 196 BNS) are covered by both the IPC and the BNS. These rules are intended to prevent the abuse of internet platforms for illegal purposes.

Accountability of Social Media Platforms
Obligations under the IT Act and Rules

Significant Social Media Intermediaries (SSMIs) must register in accordance with stricter due diligence regulations, which include hiring a chief compliance officer and conducting frequent audits.

Grievance Redressal: In order to ensure prompt action against illegal material, platforms are required to reply to user complaints within 15 days.

- **Content Moderation:** It is important to detect and neutralise dangerous information using both artificial intelligence and human review techniques.

Judicial Interpretation
1. Constitutional Safeguards and Free Speech

In Shreya Singhal v. Union of India [12] (2015), the Supreme Court ruled that Section 66A of the IT Act, 2000 was unconstitutional, highlighting the need of striking a balance between appropriate internet limitations and free expression. The ruling emphasised that ambiguous and expansive clauses might be abused, shielding people from capricious censorship.

2. Intermediary Liability

The obligations of intermediaries under Section 79 of the IT Act were reviewed in the Google India Pvt. Ltd. v. Visaka Industries (2020) case. The "safe harbour" concept was defined by the court, which mandated that platforms take prompt action when they became aware of illegal material. Indian courts have made it clear time and time again that intermediaries cannot claim immunity if they disregard legal obligations, such content removal orders.

3. Data Privacy and Surveillance

The important ruling in Justice K.S. Puttaswamy v. Union of India [13] (2017) acknowledged privacy as a fundamental right under Article 21 of the Constitution, which has an impact on how courts interpret data protection in the digital sphere. Since then, courts have examined how social media companies gather, store, and utilise user data to make sure privacy laws are being followed.

Challenges and Gaps
1. Ambiguity in Laws

There is uncertainty about the scope of intermediary liability due to the wide phrasing of several clauses of the IT Act and the 2021 Rules. To avoid abuse and guarantee equitable enforcement, courts and legislators need to make these rules clear.

f Law

2. Enforcement Issues

Effective investigation and prosecution of cybercrimes are hampered by law enforcement agencies' limited resources and technological skills. Enforcement activities are made more difficult by the absence of cooperation among different parties.

3. Privacy vs. Accountability

Concerns over user privacy have been highlighted by the 2021 Rules' need to track down the creators of illegal material. In the Indian legal system, striking a balance between these conflicting interests is still a difficult task.

Comparative Analysis: Lessons from Other Jurisdictions

Germany: Social media companies are required under the Network Enforcement Act (NetzDG) to delete unlawful information within 24 hours of being notified. Heavy penalties are imposed for noncompliance, indicating a strict attitude to intermediary responsibility.

- **Australia:** One example of centralised regulatory supervision is the Online Safety Act 2021, which gives the eSafety Commissioner the authority to request the removal of hazardous information.

These examples demonstrate India's need for strong enforcement systems and precise legal directives.

- .

Recommendations

1. Comprehensive Legislation

The existing fragmented approach should be replaced by a single legislative framework that addresses cybercrime, intermediary responsibility, and user rights.

2. Capacity Building

To combat the ever-changing nature of cybercrimes, law enforcement authorities need to be trained and equipped with cutting-edge technologies. Working together with academics and IT specialists may improve investigative skills.

3. Public Awareness

Users may be empowered to identify and report cybercrimes via awareness programs on digital literacy and safe online habits. These initiatives may be strengthened via collaborations with NGOs and academic institutions.

Conclusion

Cybercrime on social media platforms must be addressed as India moves closer to a digital future. Social media may continue to be a vehicle for empowerment rather than exploitation with the help of a strong legal framework, careful enforcement, and cooperation among parties.

References

1. Bhatt K. Cybercrime: India's Digital Dark Side. The Hindu, August 15, 2021, 7.
2. Seth K. New Technology Laws, Computers, and the Internet. LexisNexis, c2021, pp. 125-135.
3. Gupta A. An Overview of Safe Harbour Provisions and Intermediary Liability in India. Indian J Law Technol. 2019; 8:45-59.
4. Bhatia G. Indian Judicial Reactions to Free Speech and Social Media Regulation. Econ Polit Weekly, 56(3), 25–30, 2021.
5. Write Civil Petition No. 845 of 2021.
6. Bhatt K. Cybercrime: India's Digital Dark Side. The Hindu, August 15, 2021.
7. Duggal P. Cyber Law: The Indian View. Universal Law Publishing, c2020, pp. 89-102.
8. Suo Moto Writ (Criminal) No. 3 of 2015.
9. Recognising the New IT Regulations. The Indian Express, March 10, 2021.
10. Seth K. New Technology Laws, Computers, and the Internet. LexisNexis, c2021, p. 215.
11. Gupta A. An Overview of Safe Harbour Provisions and Intermediary Liability in India. Indian J Law Technol. 2019; 8:45. 12.AIR 2015 SC 1523
13. SC 4161 AIR 2017