ISSN: 2393-8048
International Advance Journal of Engineering, Science and Management (IAJESM)
Multidisciplinary, Multilingual, Indexed, Double Blind, Open Access, Peer-Reviewed, Refereed-International Journal.
SJIF Impact Factor =8.152, July-December 2025, Submitted in July 2025

Cyber Crimes in the Age of Social Media: An Indian Perspective

Khushboo Singla, Research Scholar, Dept. of Law, Shri Khushal Das University, Hanumangarh (Rajasthan)
Dr. Vikram, Research Supervisor, Dept. of Law, Shri Khushal Das University, Hanumangarh (Rajasthan)

Abstract

The rapid expansion of social media platforms has transformed communication, commerce, and social interaction in India. Alongside these benefits, the digital ecosystem has also facilitated a sharp rise in cyber-crimes, ranging from identity theft and online fraud to cyberstalking, misinformation, and hate speech. This paper examines the nature, scope, and impact of cyber-crimes associated with social media usage in India. It analyzes prevailing trends, legal frameworks, enforcement challenges, and preventive strategies, offering an Indian perspective grounded in socio-legal realities. The study aims to contribute to policy discourse and public awareness by identifying gaps in regulation and proposing actionable measures for safer digital engagement.

Keywords: Cyber Crime, Social Media, India, Information Technology Act, Online Safety

Introduction

The advent of social media has fundamentally altered the way individuals interact, share information, and participate in public discourse. Platforms such as Facebook, Instagram, X (formerly Twitter), WhatsApp, and YouTube have become integral to daily life in India, a country with one of the world's largest internet user bases. While these platforms enable connectivity and democratize information, they also provide fertile ground for cyber criminals to exploit vulnerabilities.

Cyber-crimes committed via social media are particularly concerning due to their scale, anonymity, and speed of dissemination. The increasing dependence on digital platforms for communication, education, governance, and commerce has amplified the potential harm caused by such crimes. This paper explores cyber-crimes in the age of social media with a specific focus on India, examining their forms, causes, legal responses, and preventive mechanisms.

Literature Review

Malik and Choudhury (2018) examine the policy landscape in India addressing cyber-crime, emphasizing the need for adaptive legal and institutional mechanisms in response to rapidly evolving digital threats. Their study highlights gaps in enforcement capacity, inter-agency coordination, and public awareness, arguing that legislation alone is insufficient without robust implementation and continuous policy updates. The authors underscore the importance of aligning cyber-crime policies with technological advancements and international best practices, particularly in the context of social media platforms where anonymity, scale, and cross-jurisdictional operations complicate regulation. Their work provides a foundational policy-oriented perspective that informs the present study's focus on social media–enabled cyber-crimes in India, especially regarding the role of governance frameworks, stakeholder collaboration, and preventive strategies.

Conti, Poovendran, and Secchiero (2012) focus on the technical dimensions of cyber-crime prevention through their study on detecting fake profiles in online social networks. The authors propose analytical and algorithmic techniques to identify fraudulent and deceptive accounts, highlighting how fake profiles are central to crimes such as identity theft, online fraud, and social engineering. Their work is particularly relevant in the Indian social media context, where large user bases and limited verification mechanisms make platforms vulnerable to impersonation and misuse.

Asur (2010), through research conducted at the Social Computing Lab, HP Labs, explores the predictive power of social media data in understanding future trends and collective behavior. While the study primarily emphasizes opportunities in social media analytics, it also implicitly reveals risks associated with data misuse, manipulation, and surveillance. The findings

underscore how predictive capabilities of social media can be exploited by malicious actors, thereby contributing to emerging forms of cyber-crime and information warfare.

Conceptual Framework of Cyber Crime

Cyber-crime refers to unlawful activities conducted using computers, digital devices, or networks, where the computer may be the target, tool, or place of crime. In the context of social media, cyber-crimes often involve misuse of personal data, impersonation, harassment, and manipulation of digital content.

Social media–related cyber-crimes can be broadly categorized into:

- Crimes against individuals (cyberstalking, bullying, defamation)
- Crimes against property (identity theft, financial fraud)
- Crimes against society and the state (fake news, hate speech, cyber terrorism)

The interactive and user-generated nature of social media intensifies these risks, making regulation and enforcement complex.

Types of Cyber Crimes on Social Media in India

Cyber-crimes on social media in India manifest in diverse forms, reflecting the complex interaction between technology and human behavior. One of the most prevalent forms is identity theft and impersonation, where offenders create fake profiles using stolen personal information to deceive users and commit fraud. Cyberstalking and online harassment, particularly targeting women and minors, involve persistent abuse, threats, and intimidation through messages, comments, and posts. Online financial fraud has increased significantly with the use of phishing links, fake advertisements, and fraudulent investment schemes circulated through social media platforms. Another serious concern is the spread of misinformation and fake news, which has led to social unrest, public panic, and erosion of trust in democratic institutions. Cyber defamation and hate speech are also widespread, where false, offensive, or inflammatory content is used to damage reputations or incite communal disharmony. Additionally, non-consensual sharing of images and videos, including morphed content, violates personal privacy and dignity. Collectively, these cyber-crimes highlight the growing misuse of social media in India and underscore the urgent need for effective legal regulation, technological safeguards, and digital awareness initiatives.

Identity Theft and Impersonation

Identity theft and impersonation are among the most common cyber-crimes on social media in India. Cyber criminals create fake profiles by misusing stolen personal information, photographs, or credentials of individuals to gain trust and deceive others. Such impersonation is frequently employed to conduct financial fraud, extract sensitive information, or manipulate victims through social engineering techniques. In many cases, offenders pose as friends, relatives, or officials to solicit money or confidential data, causing financial loss and reputational harm to victims. The widespread use of social media platforms and limited user awareness further aggravate the prevalence of this form of cyber-crime in the Indian digital landscape.

Cyberstalking and Online Harassment

Cyberstalking and online harassment refer to the persistent and unwanted use of digital communication to intimidate, threaten, or emotionally distress individuals. In the Indian context, women and minors are particularly vulnerable to such offenses on social media platforms. Harassment commonly takes the form of abusive or obscene messages, repeated unwanted contact, threats, trolling, and the non-consensual sharing of images or personal information. These acts not only violate personal privacy but also have serious psychological and social consequences for victims, including fear, anxiety, and social withdrawal. The anonymity provided by social media and inadequate reporting mechanisms further exacerbate the prevalence of cyberstalking and online harassment, highlighting the need for stronger legal enforcement and greater digital awareness.

Online Fraud and Financial Scams

Online fraud and financial scams have witnessed a significant rise in India due to the extensive use of social media platforms. Cyber criminals exploit these platforms to circulate phishing links, promote fake investment schemes, and publish fraudulent advertisements that lure unsuspecting users with promises of quick profits or discounted products. The growing integration of social media with digital payment systems and online banking has further heightened financial risks, enabling offenders to execute transactions swiftly and anonymously. Such scams often result in substantial monetary losses and erode public trust in digital platforms. The lack of adequate user awareness and delayed reporting mechanisms continue to pose major challenges in effectively addressing online financial fraud in the Indian context.

Misinformation and Fake News

The rapid spread of misinformation through social media poses serious social and political challenges in India. Fake news has been linked to public panic, communal tension, and erosion of trust in institutions.

Cyber Defamation and Hate Speech

Defamatory content and hate speech circulate widely on social media, often targeting individuals, communities, or public figures. Such content can incite violence and disrupt social harmony.

Legal Framework Governing Cyber Crimes in India

Information Technology Act, 2000

The Information Technology Act, 2000 (IT Act), along with its amendments, forms the backbone of cyber law in India. Provisions such as Sections 43, 66, 66C, 66D, and 67 address unauthorized access, identity theft, cheating by personation, and publication of obscene content.

Indian Penal Code, 1860

Several provisions of the Indian Penal Code (IPC), including Sections 354D (stalking), 499 (defamation), 503 (criminal intimidation), and 509 (insulting the modesty of a woman), are applied to cyber-crimes committed via social media.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

These rules impose due diligence obligations on social media intermediaries, including grievance redressal mechanisms, content takedown requirements, and accountability measures.

Challenges in Combating Social Media–Related Cyber Crimes

Despite the existence of legal provisions, several challenges hinder effective control of cyber-crimes in India:

- Anonymity and pseudonymity of users
- Jurisdictional issues in cross-border crimes
- Lack of digital literacy and awareness
- Underreporting of cyber crimes
- Limited technical capacity of law enforcement agencies

These challenges necessitate a multidimensional approach involving legal, technological, and educational interventions.

Preventive and Control Measures

Effective prevention and control of cyber-crimes on social media in India require a comprehensive approach involving legal, technological, institutional, and social interventions. Strengthening the existing legal framework through timely amendments and strict enforcement of cyber laws is essential to deter offenders and ensure accountability. Law enforcement agencies must be equipped with advanced technical infrastructure and specialized training to investigate cyber-crimes efficiently. Social media platforms play a crucial role by implementing robust content moderation policies, user verification mechanisms, and prompt

grievance redressal systems. Promoting digital literacy and public awareness through educational institutions, government initiatives, and media campaigns can empower users to recognize cyber threats and adopt safe online practices. Additionally, the use of advanced technologies such as artificial intelligence and data analytics can aid in early detection of fraudulent activities and harmful content. Collaborative efforts among government bodies, private platforms, civil society, and users are vital for creating a secure and responsible social media environment in India.

Strengthening Legal and Institutional Mechanisms:

Strengthening legal and institutional mechanisms is essential for the effective prevention and control of cyber-crimes in India. Regular updating of cyber laws is necessary to keep pace with rapidly evolving technologies and emerging forms of social media–related offenses. Capacity building of cyber-crime cells through specialized training, modern forensic tools, and adequate staffing can significantly improve investigation and prosecution rates. Additionally, faster judicial processes and dedicated cyber courts can enhance deterrence by ensuring timely justice for victims.

Role of Social Media Platforms:

Social media platforms play a pivotal role in addressing cyber-crimes by adopting robust content moderation policies and proactive monitoring systems. Enhancing user verification mechanisms can help reduce fake profiles and impersonation. Platforms must also cooperate with law enforcement agencies by sharing relevant information in a lawful and transparent manner, while simultaneously respecting user privacy and freedom of expression. Effective grievance redressal systems are crucial for prompt removal of harmful content.

Public Awareness and Digital Literacy:

Promoting digital literacy is a key preventive strategy in combating cyber-crimes on social media. Educational institutions, government agencies, and civil society organizations should conduct awareness programs and public campaigns to educate users about online safety, privacy protection, and reporting mechanisms. An informed user base is better equipped to identify cyber threats, avoid falling victim to scams, and report cyber-crimes in a timely manner.

Technological Solutions:

The use of advanced technological solutions such as artificial intelligence, machine learning, and data analytics can significantly enhance cyber-crime detection and prevention. These technologies can assist in identifying suspicious patterns, detecting fake accounts, and curbing the spread of misinformation and malicious content. Integrating such tools into law enforcement systems and social media platforms can improve early warning mechanisms and strengthen overall cyber security in the digital ecosystem.

Conclusion

Cyber-crimes in the age of social media represent a significant challenge for India's digital future. While social media platforms have become indispensable tools for communication and expression, their misuse poses serious risks to individuals and society. Addressing these challenges requires a balanced approach that safeguards fundamental rights while ensuring accountability and security. Strengthening legal frameworks, enhancing institutional capacity, fostering cooperation between stakeholders, and promoting digital awareness are crucial steps toward creating a safer social media environment in India.

References

1. Sites, S. N. (2020). A Critical Appraisal of Crime Over Social Networking Sites in the Context of India.
2. Malik, J. K., & Choudhury, S. (2018). Policy Considerations in India Against Cyber Crime. International Journal of Recent Scientific Research, 9(12), 29811-29814.
3. GANESH, S., GANAPATHY, D., & SASANKA, K. (2020). Awareness of Cyber Crime

on Social Media. The journal of contemporary issues in business and government, 26(2), 1758-1765.

4. Chakraborty, S., &Kusuman, S. (2014). Critical Appraisal of Information Technology Act. Academike, Articles on Legal Issues.
5. Halder, D., & Jaishankar, K. (2016). Cyber victimization in India: A baseline survey report (2010). SSRN Electronic Journal. https://doi.org/10.2139/ ssrn.1759708
6. Halder, D., & Jaishankar, K. (2017). Cyber Crimes Against Women in India. Sage Publications, New Delhi.
7. Joshi, Y., & Singh, A. (2013). A study on cyber-crime and security scenario in India. International Journal of Engineering and Management Research, 3(3), 13-18.
8. Khanna, P. (2015). New Media Technologies: Impact on Adolescents. Communication Today, 214-223.
9. Kinley, P. (2016). Data Analytics for Beginners: Basic Guide to Master Data Analytics. CreatSpace.
10. Ray, S., & Ghoshal, A. (2016, August 25). Every sixth cybercrime in India committed through social media. Hindustan Times.
11. Riva, G., Wiederhold, B. K., &Cipresso, P. (2016). The Psychology of Social Networking: Identity and relationships in online communities. De Gruyter Open.
12. Tomalin, S. (2017, November 24). What effect is social media having on society? Umi Digital. Retrieved January 6, 2021, from https://umidigital.co.uk/blog/affect-social-media-society/
13. Conti M., Poovendran R., Secchiero M., Fakebook: Detecting fake profiles in on-line social networks, Proceedings of the International Conference on Advances in Social Networks Analysis and Mining (2012).
14. SitaramAsur Social Computing Lab HP Labs Palo Alto, California 2010 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology: "Predicting the Future WithSocial Media".
15. Dimensions against Cyberviolence in India." Computers in Human Behavior 25.5: 1089-1101.
16. Dubey, Pushkar, and Srijan Pateriya. "Social Media and Cybercrime: A Sociodemographic Study of Awareness Level Among Indian Youth." Cybercrime in Social Media. Chapman and Hall/CRC 23-40.