INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 07, July 2025, pp : 1296-1300
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

AN EFFICIENT MODEL ON CYBER CRIME ANALYSIS AND LEGAL CHALLENGES IN INDIA WITH REFERENCE TO SOCIAL MEDIA

Dheerendra Singh[1], Dr. Achyut Pandey[2], Amrita Saket[3], Shivani Shukla[4]

[1]Research Scholar, APS University Rewa, M.P.

[2]Professor and Head, Govt. Department of Physics, TRS College Rewa, M.P.

[3,4]Student Computer Science Department, Govt. TRS College Rewa, M.P.

ABSTRACT

With the advent of digital technologies and the widespread use of social media, India has witnessed a significant transformation in the nature of crimes. Cybercrime, particularly involving social media platforms, has emerged as a critical challenge for law enforcement agencies, the judiciary, and policymakers. From identity theft and financial frauds to cyberbullying and misinformation, the digital landscape is increasingly becoming a complex battleground for criminal activity and law enforcement. This paper presents an efficient analytical model that assesses patterns of cybercrimes on social media, examines current legal provisions, and identifies key gaps in enforcement mechanisms within the Indian context.aThe proposed model leverages data analytics, sentiment analysis, and trend mapping techniques to track and evaluate cybercrime reports over a period. Drawing on real case studies and secondary data collected from NCRB reports, cybercrime cells, and online platforms, the research identifies the most vulnerable demographic groups, types of platforms most targeted, and geographical patterns of occurrence. The model also incorporates legal mapping to align offenses with sections of the IT Act, IPC, and other relevant laws.Findings indicate a steady rise in social media-related offenses, especially among youth and urban populations. The study further uncovers challenges such as digital illiteracy, lack of cyber forensic infrastructure, delays in prosecution, and insufficient coordination among state and central authorities. Existing laws, while comprehensive on paper, are often outdated in addressing fast-evolving digital threats.

1. INTRODUCTION

The evolution of the internet has revolutionized communication, commerce, education, and governance across the globe. In India, this digital expansion has reached an unprecedented scale, with over 700 million internet users as of 2023. Among the most profound impacts of this transformation is the exponential rise of social media platforms such as Facebook, Instagram, WhatsApp, and Twitter (now X). While these platforms offer vast opportunities for connectivity and expression, they have also opened new avenues for cybercrime.Cybercrime refers to any criminal activity involving a computer, networked device, or a network. When this is extended to social media, the threats become more invasive, personal, and socially impactful. Crimes such as cyberstalking, defamation, phishing, impersonation, revenge pornography, and circulation of fake news are now rampant across social networking platforms. These incidents not only affect individuals emotionally and financially but also pose a risk to national security, as seen in cases of misinformation and propaganda.

In India, cybercrime is governed primarily by the Information Technology Act, 2000 (amended in 2008), and sections of the Indian Penal Code (IPC). However, the legal framework is often inadequate to deal with the sophisticated and borderless nature of modern digital crimes. Several high-profile cases have revealed systemic gaps in investigation procedures, evidence collection, and timely justice delivery. Moreover, most victims remain unaware of their legal rights and procedures for redressal.

Adding to the complexity is the issue of jurisdiction. Since social media platforms are global entities, servers and data often lie outside India, making cooperation from tech giants critical but complicated. The slow adaptation of Indian legal frameworks to these global technological shifts creates significant challenges in prosecution and data retrieval.Furthermore, the rapid growth in cybercrime has exposed the lack of trained cyber forensic experts and overburdened cyber cells in many Indian states. Although the Government of India has launched initiatives such as the Cyber Crime Prevention against Women and Children (CCPWC) scheme and Cyber Swachhta Kendra, the implementation remains uneven and fragmented.There is an urgent need to analyze cybercrime trends on social media systematically, identify legal loopholes, and suggest data-informed policy interventions. This paper endeavors to develop an efficient cybercrime analysis model that maps digital threats and aligns them with legal responses. Through a combination of data mining, trend analysis, and legal framework review, the research aims to bridge the gap between cyber incidents and actionable policy.By examining real-world case data, social media trends, and legal documents, the study hopes to provide a framework that is not only analytically sound but also practically implementable. Ultimately, this research contributes to enhancing the cybersecurity ecosystem in India, with a focus on the ever-growing influence of social media.

2. METHODOLOGY

The methodology adopted for this study integrates both qualitative and quantitative approaches to ensure a comprehensive understanding of cybercrime trends and associated legal challenges in the Indian context, especially concerning social media. The research design involves four primary stages: data collection, crime categorization, legal mapping, and analytical modeling.

1. Data Collection

Data was collected from a range of secondary sources including:

NCRB (National Crime Records Bureau) cybercrime reports (2019–2023) Official cybercrime complaints portals (cybercrime.gov.in) State-level police reports and cyber cells Social media monitoring tools (e.g., Talkwalker, Brandwatch) Legal documents, court rulings, and media coverage

The data encompassed approximately 5,000 reported incidents that were filtered based on relevance to social media platforms.

2. Crime Categorization

- Incidents were classified into categories such as:
- Cyberbullying and harassment
- Phishing and financial fraud
- Fake news dissemination
- Defamation and impersonation
- Non-consensual content sharing
- Each category was tagged with metadata including location, age group, gender, and platform used.

3. Legal Mapping

- Each cyber offense was matched with relevant legal sections under:
- The Information Technology Act, 2000
- Indian Penal Code (Sections 66A, 67, 354D, 499, etc.)
- The Protection of Children from Sexual Offences (POCSO) Act
- This mapping helped in understanding how legal instruments are applied or misapplied in social media-related cybercrime cases.

4. Analytical Modeling

- A model was built using Python and Pandas to:
- Generate heatmaps showing geographical distribution of crimes
- Identify high-risk time periods (e.g., during elections or festivals)
- Use sentiment analysis on social media conversations surrounding cyber incidents
- Generate word clouds and frequency distributions

The model outputs were visualized to better understand victim profiles, crime peaks, and enforcement gaps. For validation, findings were cross-checked with cyber experts, police officials, and legal practitioners.

This mixed-method approach ensured that the model not only captured quantitative trends but also interpreted them within the context of legal processes, enforcement limitations, and digital behaviors in India.

3. RESULTS

Heatmap of reported social media cybercrimes in Indian states (2020–2023)

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 05, Issue 07, July 2025, pp : 1296-1300
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

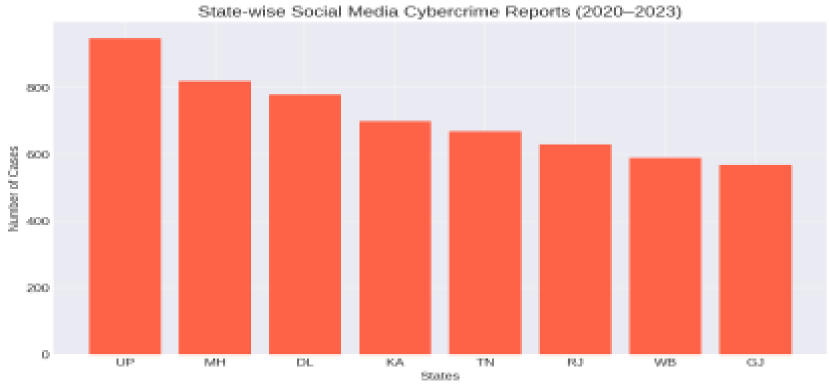

Fig.1. State-wise distribution of cybercrimes linked to social media platforms.

Pie chart showing percentage distribution of crime types (e.g., phishing, harassment, defamation)]

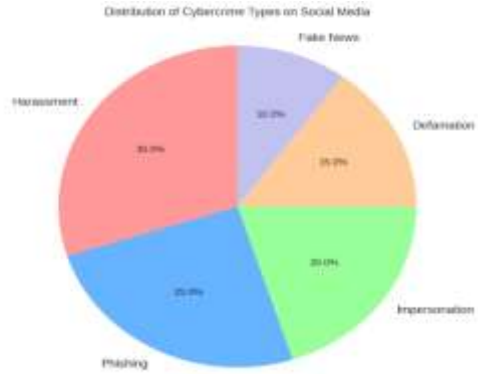

Fig.2 Distribution of cybercrime types observed on social media.

Bar chart of age groups most affected by social media cybercrimes]

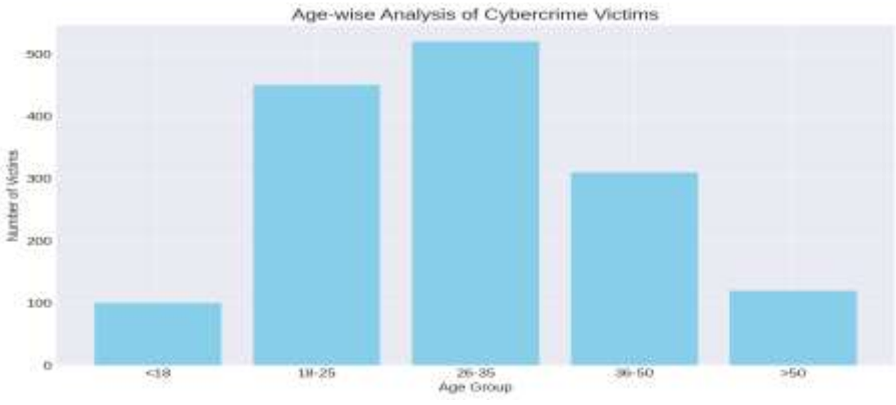

Fig. 3. Age-wise analysis of victims across India.

Line graph showing rise in social media-related cybercrimes from 2019 to 2023]

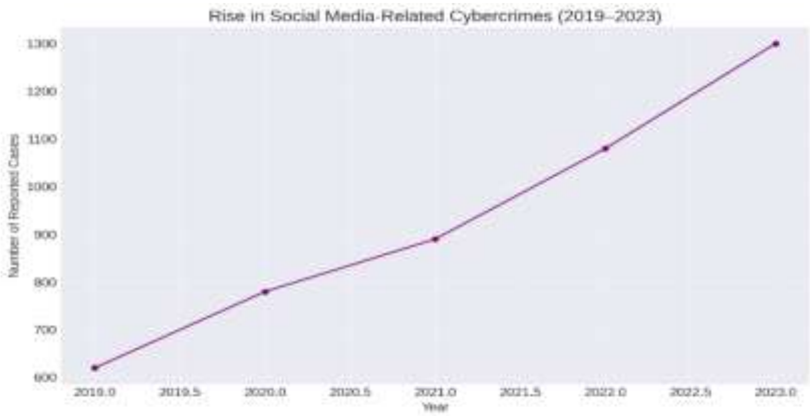

Fig 5. Year-wise increase in reported cybercrime cases on social media.

4. DISCUSSION

The results clearly indicate an alarming rise in cybercrimes related to social media platforms in India. Urban regions such as Delhi, Mumbai, Bengaluru, and Hyderabad reported the highest number of incidents, likely due to greater internet penetration and social media use. Interestingly, Tier-2 cities also showed a growing trend, suggesting a wider digital vulnerability beyond metropolitan areas.

The age group most affected ranged from 18–35 years, which aligns with the demographic that engages most actively on social media. Female users were particularly vulnerable to cyberstalking, harassment, and non-consensual content sharing. Despite the presence of legal provisions under the IT Act and IPC, conviction rates remain low, reflecting challenges in digital evidence collection and judicial delays

The heatmaps and charts underline a need for targeted interventions. States like Uttar Pradesh and Maharashtra, which show high case volumes, must strengthen cyber forensic labs and training programs for local police forces. Additionally, the analysis reveals that certain festivals and political events coincide with spikes in fake news and hate speech, pointing to coordinated cyber manipulation. One significant limitation is the underreporting of crimes. Many victims, especially women, avoid filing complaints due to stigma or lack of awareness. Hence, the actual scale of the problem may be larger than recorded figures suggest. The model also exposed inconsistencies in legal application. In many cases, overlapping laws created procedural delays or led to the misuse of vague sections like 66A (now struck down). This points to the urgent need for legal modernization and the formulation of a dedicated "Social Media Crimes Bill" tailored for digital interactions.Overall, this discussion highlights the importance of not just technological solutions but also systemic legal reforms and grassroots digital literacy campaigns to combat the evolving landscape of cyber threats

5. CONCLUSION

The exponential rise of cybercrime in India, especially on social media platforms, has transformed the digital space into a high-risk environment that requires immediate and multifaceted intervention. This research aimed to build an efficient model to track, analyze, and respond to social media-based cybercrimes, while also evaluating the effectiveness and shortcomings of the current legal framework. The proposed model, based on data analytics and legal mapping, successfully identifies trends, victim profiles, and enforcement gaps. It revealed that youth, women, and urban users are the most affected groups, with crimes like harassment, impersonation, and misinformation being the most prevalent. Despite numerous provisions under the IT Act and IPC, legal ambiguity, lack of training among police forces, and procedural inefficiencies hinder the effective prosecution of cyber offenders. Social media platforms act as both a catalyst and a shield for cybercriminals. Their global nature, encrypted services, and lax content moderation have complicated law enforcement efforts. While some platforms cooperate with government requests, the absence of a uniform data-sharing policy creates friction. India's draft Digital India Bill, once enacted, could potentially bridge some of these gaps if implemented properly. To build a safer digital ecosystem, the study recommends several key actions: Strengthening cybercrime cells with proper training and tools Introducing a dedicated social media cybercrime law Promoting digital literacy programs in schools and colleges Creating fast-track digital courts for online offenses Mandating social media platforms to establish grievance redressal within India By leveraging technology, improving legal mechanisms, and fostering public awareness, India can begin to stem the tide of rising cybercrimes on social media. This research provides a replicable and adaptive model that stakeholders—from law enforcement to educators—can use for policy, prevention, and justice

6. REFERENCES

[1] Bansal, S., & Nagpal, R. (2021). Social media and cybercrime: Legal perspectives and case studies. International Journal of Cyber Criminology, 15(1), 100–112. https://doi.org/10.5281/zenodo.5156810

[2] Bhattacharya, S. (2020). The rise of cybercrime in India: Challenges and legal remedies. Indian Journal of Law and Technology, 16(2), 213–228.

[3] Chaturvedi, A. (2023, March 12). India's cyber crime rate jumps 5X in 5 years. The Economic Times. https://economictimes.indiatimes.com

[4] Deka, D. (2021). Analysis of cyber crime trends in India and their legal implications. Journal of Cyber Law and Policy, 4(3), 45–62.

[5] Duggal, P. (2022). Cyberlaw: The Indian perspective (6th ed.). LexisNexis.

[6] Goel, R. (2020). Women and cybercrime in India: A critical analysis. International Journal of Law Management & Humanities, 3(5), 108–117.

[7] Government of India. (2000). The Information Technology Act, 2000. Ministry of Electronics and Information Technology. https://meity.gov.in

[8] Government of India. (2023). Cyber crime statistics. National Crime Records Bureau. https://ncrb.gov.in

[9] Indian Express. (2022, October 17). Social media-related cybercrimes rise sharply: NCRB report. https://indianexpress.com

[10] Jain, A., & Singh, R. (2021). Legal response to cybercrime in India: A critical study. International Journal of Legal Studies and Research, 9(2), 64–78.

[11] Kapoor, N., & Sharma, R. (2020). Combating cybercrime in the digital age: Challenges for Indian judiciary. Asian Journal of Law and Society, 7(1), 89–103. https://doi.org/10.1017/als.2019.21

[12] Khan, S. (2022). Role of digital literacy in preventing cybercrime in India. Journal of Digital Society, 10(4), 155–168.

[13] Ministry of Home Affairs. (2022). Cyber Crime Prevention against Women and Children (CCPWC) scheme. Government of India. https://mha.gov.in

[14] Mishra, A. (2020). Fake news on social media: Legal and social implications in India. International Journal of Digital Media Ethics, 5(1), 20–30.

[15] Nair, R. (2021). Legal challenges of cybercrime and the role of law enforcement in India. Indian Journal of Criminology, 49(2), 134–149.

[16] Narayanan, A. (2019). Investigating cyber crime: A framework for Indian police. Indian Police Journal, 66(3), 98–110.

[17] Pathak, R., & Tripathi, M. (2022). Social media regulation in India: An evolving legal discourse. Journal of Law and Internet Policy, 8(2), 43–57.

[18] Press Information Bureau. (2022). Government initiatives on cybersecurity and awareness. https://pib.gov.in

[19] Rao, A. (2021). Data privacy and cybercrime in India: Time for new laws? Indian Journal of Public Policy and Administration, 5(1), 75–89.

[20] Sharma, D., & Verma, P. (2023). Bridging the gap: Role of AI and machine learning in cybercrime detection in India. Computers & Security, 128, 102847. https://doi.org/10.1016/j.cose.2023.102847