

A Comparative Study of Cybercrime Cases on Social Media in India: Technical and Legal Aspects

¹Dheerendra Singh Patel, ¹Department of Computer Science, APSU Rewa M.P.

E-mail: dheerendras153@gmail.com

²Dr. Achyut Pandey, ²Professor and Head Department of Physics and Computer Science,
Govt. TRS College Rewa M.P, Email: achyut.pandey9@gmail.com

³Sonam Singh, ³Department of Computer Science, Govt. TRS College Rewa M.P.

⁴Preeti Tiwari, ⁴Department of Computer Science, Govt. TRS College Rewa M.P.

Abstract

In the wake of India's accelerating digital transformation, social media has emerged as both a powerful tool for communication and a vulnerable frontier for cybercriminal activity. Utilizing secondary data from the National Crime Records Bureau (NCRB), legal statutes, and scholarly literature, the research traces the sharp rise in platform-specific cybercrime cases from 2018 to 2023. Facebook and Instagram appear most frequently in incident data, followed by WhatsApp and Twitter, reflecting broader patterns in user behaviour and attacker exploitation. Through trend analysis and visual representation, the study not only maps the escalation of social media-related offenses but also evaluates the robustness and limitations of existing legal instruments such as the Information Technology Act, 2000. The findings highlight critical gaps in enforcement, the need for adaptive legal reform, and the urgency of cross-sector collaboration to safeguard India's digital public sphere.

Keywords: Social Media Cybercrime, Digital Offenses in India, Cyber Law and IT Act, NCRB Trend Analysis, Platform-Specific Vulnerabilities

Introduction

In the digital age, social media has emerged as one of the most transformative innovations, reshaping the ways individuals communicate, share information, express opinions, and engage with society. Platforms such as Facebook, Twitter, Instagram, and WhatsApp have become integral to daily life for millions in India, offering unprecedented connectivity and opportunities for free expression. However, this pervasive integration has also brought with it an alarming increase in cybercrime activities, particularly on these platforms. With India ranking among the world's top consumers of social media, the country has

witnessed a corresponding rise in cybercrime cases, ranging from online harassment, identity theft, cyberstalking, trolling, defamation, financial fraud, and the dissemination of sexually explicit content, to misinformation and hate speech. The scope and complexity of these offenses have evolved with technological advancements, posing serious threats to personal safety, privacy, democratic discourse, and national security.

The vast user base and minimal entry barriers of social media platforms have made them fertile ground for both petty and organized cybercriminal activities. The anonymity afforded by the internet, coupled with weak digital literacy and limited enforcement capabilities, exacerbates the problem, allowing perpetrators to evade detection and punishment. In India, incidents such as the online targeting of public figures, revenge porn, phishing scams, fake news propagation leading to mob lynching, and coordinated misinformation campaigns during elections have gained national and international attention. These instances underscore the urgent need for a detailed and interdisciplinary investigation into the patterns, mechanisms, and responses associated with social media-related cybercrimes. While various reports and agencies have acknowledged the exponential rise of such offenses, a comprehensive comparative study focusing on both the technical and legal dimensions remains scarce.

From a technical perspective, detecting and mitigating cybercrime on social media requires sophisticated mechanisms, including machine learning algorithms, natural language processing (NLP), sentiment analysis, and network analysis. With the majority of abusive or harmful content embedded in code-mixed, multilingual, or image-based formats, conventional detection systems often fall short in the Indian context. Moreover, the dynamic and real-time nature of social media demands automated and scalable solutions that can filter, flag, or block malicious activity without compromising user experience or freedom of speech. Platforms like Meta (formerly Facebook), X (formerly Twitter), and YouTube have adopted AI-based moderation systems; however, their efficacy in the Indian sociocultural and linguistic context is questionable due to algorithmic bias, lack of contextual understanding, and regional disparities in content moderation infrastructure. A comparative analysis of the technical strategies employed in cybercrime detection can reveal critical gaps and opportunities for innovation in designing localized, context-aware, and ethically sound technological solutions.

Simultaneously, the legal and regulatory response to cybercrimes on social media in India is complex and continually evolving. The primary legal framework governing cybercrime includes the Information Technology Act, 2000 (amended in 2008), and various provisions of the Indian Penal Code (IPC), such as Sections 354D (cyberstalking), 499 (defamation), and 507 (criminal intimidation via electronic communication). Additionally, the Personal Data Protection Bill, though still pending as of recent debates,

aims to strengthen data governance and user protection. However, challenges remain in the implementation, interpretation, and enforcement of these laws. Jurisdictional ambiguities, procedural delays, lack of digital forensic capabilities, and limited awareness among police and judiciary often hinder the timely prosecution of cybercrime cases. High-profile cases such as the "Bois Locker Room" controversy, the online harassment of journalists and activists, and manipulated media shared during political elections reflect the gaps in India's current cyber legal framework and highlight the need for a more robust and adaptive legal system that can effectively address emerging threats.

A comparative study of cybercrime cases reveals significant differences in the way these incidents are reported, investigated, and adjudicated across different regions in India. Urban centers with advanced cybercrime cells and digital infrastructure tend to have better reporting mechanisms and response rates, while rural and semi-urban areas often lack the institutional support necessary for timely intervention. Gender, caste, and socio-economic disparities also play a significant role in determining victims' access to justice and digital safety. Women, minorities, and marginalized groups are often disproportionately targeted in online spaces, yet face systemic hurdles in pursuing legal redress. Additionally, discrepancies in how various social media platforms respond to abuse reports — based on severity, political pressure, or public attention — create inconsistencies in enforcement and accountability. By comparing multiple cybercrime cases, this study seeks to map these disparities and explore how technical mechanisms and legal responses interact or fail to converge in practice. The regulatory landscape is influenced by global debates on platform responsibility, free speech, surveillance, and user privacy. With the Indian government increasingly asserting control over digital platforms through policies like the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, tensions have emerged between state authority and corporate interests. These tensions impact the transparency and efficacy of cybercrime investigations, especially when platforms delay or resist sharing user data on grounds of jurisdiction or data privacy. This raises critical questions about accountability, user rights, and the ethical boundaries of law enforcement in digital spaces. The balancing act between safeguarding civil liberties and ensuring cybersecurity is at the heart of the legal discourse surrounding social media regulation in India. A nuanced understanding of this balance is necessary to develop policies that are both effective and rights-respecting.

The significance of this research lies in its interdisciplinary approach — integrating technical analysis of detection mechanisms with critical evaluations of legal frameworks. By comparing selected cybercrime cases on social media in India, the study aims to identify patterns in offense types, victim profiles, response mechanisms, and outcomes. It also intends to evaluate the strengths and limitations of existing tools and laws, and suggest areas for reform, innovation, and collaboration among stakeholders, including

the government, private tech firms, civil society, and academia. In doing so, this research contributes to the broader discourse on digital governance, online safety, and the responsible use of emerging technologies. The growing prevalence of cybercrime on social media in India reflects a complex interplay of technological advancement, legal gaps, user behavior, and socio-political dynamics. A focused, comparative analysis of such cases is essential for understanding the multifaceted nature of this threat and developing effective solutions that are contextually relevant and socially just. Through this study, we aim to not only highlight the critical challenges in detecting and prosecuting social media-related cybercrime but also propose actionable insights for improving both the technical infrastructure and legal frameworks governing India's digital ecosystem.

The emergence of new technologies such as end-to-end encryption, ephemeral messaging, and decentralized platforms has added further complexity to the cybercrime landscape. While these technologies enhance privacy and user control, they also present significant challenges for law enforcement agencies attempting to trace perpetrators or gather digital evidence. Messaging platforms like WhatsApp, Signal, and Telegram — widely used in India — are frequently exploited to spread misinformation, conduct illegal transactions, and coordinate criminal activities without leaving a visible digital footprint. This dual-use nature of technology necessitates a nuanced approach that protects fundamental rights such as privacy and freedom of expression while enabling lawful access for legitimate investigations. Without adequate legal safeguards and technical solutions such as lawful interception protocols or metadata-based tracking, investigators often find themselves constrained in their ability to prevent or prosecute cybercrimes effectively. The generational shift in how youth engage with social media further complicates matters. Indian adolescents and young adults are among the most active users of social platforms, yet they are also the most vulnerable to cyberbullying, sextortion, online grooming, and exposure to radical content. Despite numerous awareness campaigns and digital literacy initiatives, a large segment of the population remains uninformed about the safe and ethical use of social media. Many users are unaware of their digital rights or the mechanisms available for reporting abuse. Furthermore, psychological and social factors — such as fear of stigma, lack of trust in law enforcement, or normalization of online harassment — often lead to underreporting of cybercrimes. This underreporting distorts official statistics and impairs the development of data-driven policy interventions. A closer look at cybercrime cases can reveal these underlying social and psychological barriers that prevent justice and support a more inclusive strategy for digital safety.

In addition to individual-level harms, cybercrimes on social media can pose a broader threat to social cohesion, electoral integrity, and national security. Coordinated misinformation campaigns, foreign propaganda, deepfakes, and hate speech can polarize communities, incite violence, or manipulate public

opinion. Several incidents in India — such as the spread of communal misinformation during the Delhi riots (2020), disinformation around COVID-19, and digitally coordinated election campaigns — illustrate the scale and impact of malicious online behavior on public order and democratic institutions. These incidents often involve a blend of domestic and transnational actors, exploiting legal loopholes and jurisdictional fragmentation. The borderless nature of cyberspace demands greater international cooperation and alignment of cyber laws, data-sharing protocols, and response strategies — something India is still developing as part of its cybersecurity diplomacy efforts. From a policy standpoint, recent efforts by the Indian government to tighten social media regulation have sparked heated debates about platform accountability, data localization, and censorship. The Information Technology Rules, 2021, introduced new obligations for intermediaries, such as grievance redressal mechanisms, content takedown timelines, and traceability requirements. While these rules aim to curb online abuse and enhance user safety, they have also been criticized by digital rights groups for overreach and potential infringement on civil liberties. The effectiveness of such policies largely depends on their implementation, judicial scrutiny, and engagement with stakeholders across the spectrum. A comparative study of how these rules play out in real cybercrime cases can provide valuable insights into their practical strengths and limitations, particularly in balancing enforcement with fundamental rights.

India's federal structure adds another layer of complexity to legal enforcement in cybercrime cases. While cyber laws are primarily governed at the central level, law and order is a state subject. This division often leads to coordination challenges between state police forces and central agencies like the Cyber Crime Investigation Cell, CBI, and CERT-In. Discrepancies in infrastructure, expertise, and training across different states result in uneven enforcement outcomes. In many rural and small-town police stations, officers are inadequately trained in handling digital evidence, drafting cybercrime FIRs, or using forensic tools. These systemic issues create inconsistencies in how similar cases are dealt with across regions, making a comparative legal analysis especially important. Understanding such discrepancies is critical for recommending targeted capacity-building and standardization initiatives to improve the nationwide response to social media-related cybercrime.

Another aspect worth exploring is the role of social media platforms themselves as quasi-regulators. Companies like Meta, Google, and X have developed their own community standards, moderation algorithms, and reporting systems. However, the transparency and consistency of their enforcement practices remain questionable. Studies have shown that content flagged in regional languages or from marginalized groups often receives slower or no response compared to high-profile or English-language cases. Moreover, platforms are often reluctant to disclose how their algorithms prioritize, suppress, or amplify content — citing trade secrecy. This opacity poses a serious challenge for external accountability,

making it difficult for researchers, regulators, or civil society actors to independently assess the efficacy of moderation systems. As part of this study, examining specific cases where platform moderation either succeeded or failed can shed light on the strengths and biases of existing systems and inform recommendations for improved transparency and responsiveness.

In light of the above complexities, this research takes a multi-pronged comparative approach. It draws on real cybercrime case studies reported in different Indian states, across various social media platforms, and involving a range of legal outcomes. It compares the technical detection strategies — such as keyword-based flagging, AI moderation, and user reporting — with the legal proceedings and enforcement mechanisms applied in those cases. By doing so, the study aims to identify common patterns of failure or success, policy gaps, and areas where legal and technical systems either complement or contradict each other. It also aims to understand how sociocultural factors, victim demographics, platform policies, and state-level enforcement practices shape the outcomes of these cases.

This study, therefore, not only maps the cybercrime landscape on social media in India but also interrogates the interplay between technology, law, society, and governance. It attempts to answer critical questions: Are current detection mechanisms sufficient to deal with India's linguistic, cultural, and demographic diversity? Do the laws adequately address the realities of social media-related abuse and misinformation? How effective are social media platforms in moderating harmful content in the Indian context? And finally, how can India develop a more integrated, inclusive, and effective response to cybercrime on social media? These questions form the foundation of this comparative research, which ultimately seeks to contribute to a safer and more accountable digital environment in India.

Literature review

Amita Verma (2009) serves as a foundational text that explores the emergence and classification of cybercrimes in India within the broader legal framework. Her work provides a thorough analysis of how traditional criminal law often fails to address the complexities of digital offenses, especially those committed over social media platforms. The book highlights the loopholes in Indian cyber law enforcement and suggests the need for stronger, more specialized legal mechanisms to tackle rising cyber threats effectively.

Anirudh Rastogi focuses on the intersection of law and technology, providing insights into emerging legal challenges such as data protection, intermediary liability, and cross-border jurisdiction. In the context of social media, Rastogi's analysis is particularly relevant for understanding how Indian legal provisions like

the IT Act and privacy-related laws adapt to the fast-changing landscape of online communication and abuse. His practical approach makes it a valuable resource for both legal scholars and technology professionals.

Austin (2014) offers a conceptual foundation for understanding the applicability of traditional legal theory in the cyber domain. His principle that law is a command backed by sanctions becomes difficult to implement in borderless, decentralized environments like the internet. In analyzing cybercrimes on social media, Austin's jurisprudential framework raises key questions about how state authority and sovereignty function in digital spaces.

Albert J. Marcellai et al; (2002) offers detailed technical guidance on how to identify, preserve, and analyze digital evidence—skills critical to cybercrime investigations. In the context of social media-related offenses, the authors' focus on forensic procedures ensures that digital footprints, such as IP logs, metadata, and chat histories, can be effectively utilized in court. Their work is instrumental in bridging the gap between law enforcement practices and technological evidence-gathering techniques.

David Bainbridge (2007) provides a comprehensive overview of the legal principles governing the use of computers and digital networks. His work covers critical aspects such as copyright in software, digital contracts, data protection, and liability for computer misuse. Although rooted in the UK legal framework, Bainbridge's analysis offers valuable comparative insights for Indian cyber law discourse, especially about the regulation of user behavior on social media and the accountability of online platforms for illegal or harmful content.

D.S. Yadav (2007) is a foundational textbook that explains key concepts of IT infrastructure, software systems, and the role of the internet in modern communication. Although it is more technical, the book helps lay the groundwork for understanding how information flows through networks, which is essential when studying how cybercrimes occur and spread across social media platforms. Yadav's focus on foundational IT knowledge complements the legal discourse by providing the technical literacy necessary for interdisciplinary cybercrime research.

Research Design

The present study adopts a **descriptive and comparative research design**, which is appropriate for exploring and interpreting existing phenomena without manipulating any variables. This design allows for the systematic examination of cybercrime cases on social media platforms in India by analyzing secondary data sources. The research is focused on understanding the different types of social media-

related cybercrimes, the technical methods involved in their execution and detection, and the legal mechanisms governing such offenses. A comparative dimension is introduced by analyzing variations in trends across different regions and social media platforms, as well as in the responsiveness of legal and technical systems.

This study uses a **mixed-method approach**, combining both **quantitative** and **qualitative** elements. However, the data used is entirely based on **secondary sources**, and no primary data collection methods (such as surveys or interviews) are employed. The quantitative aspect involves analyzing crime statistics and trends, while the qualitative aspect includes the interpretation of legal texts, case studies, and technological reports related to cybercrime. The focus of the research is exploratory in nature, aiming to build a comprehensive understanding of the technical and legal challenges posed by cybercrime on social media without conducting experimental or field-based investigations.

Data Sources

The present study is entirely based on **secondary data sources**, ensuring a comprehensive understanding of cybercrime on social media from both technical and legal perspectives. One of the primary sources is the **official reports published by the National Crime Records Bureau (NCRB)**. These annual reports provide detailed statistical data on cybercrimes across India, including those specifically linked to social media platforms, enabling a data-driven analysis of trends and frequencies. In addition to statistical data, the study utilizes **judicial documents**, including case laws and court judgments accessed from authentic legal databases and official government portals. These legal texts offer valuable insights into the interpretation, prosecution, and judicial outcomes of cybercrime cases involving social media.

Data Analysis Techniques

The study primarily employs **quantitative analysis** to investigate the trends and frequency of cybercrime cases on social media platforms across India. The analysis begins with the **tabulation of data** sourced from NCRB reports and other verified secondary materials, allowing for an organized presentation of figures related to various forms of cybercrimes. This tabulated data is then translated into **graphical representations**, including **bar charts**, **pie charts**, and **line graphs**, to visually depict the fluctuations in the number and types of social media-related cybercrime incidents over a defined period. Such visual tools enhance the clarity of data interpretation and help identify patterns or anomalies in the cybercrime landscape. The study conducts **comparative analysis** across different Indian states, major cities, and commonly used social media platforms to determine geographical and platform-based vulnerabilities. This comparison aims to assess whether legal enforcement and technological safeguards vary in their effectiveness based on location or application type. Although the primary emphasis is on numerical

analysis, this approach is further enriched by **descriptive narration of landmark legal cases**, highlighting judicial responses to specific incidents. This supplementary analysis bridges the gap between numerical data and real-world legal consequences, offering a well-rounded perspective on the technical and legal aspects of cybercrime on social media.

Scope of the Study

The study focuses on the Indian context and covers cases and statistics from across the country. However, particular emphasis is placed on **regions with higher cybercrime reporting**, such as **Delhi, Maharashtra, Karnataka, Telangana, and Uttar Pradesh**. These states have recorded significant social media-related cybercrime activity, making them suitable for comparative analysis.

Data Analysis

This chapter presents a quantitative analysis of cybercrime cases related to social media platforms in India between the years **2018 and 2023**. The data, derived from secondary sources such as NCRB reports and media investigations, has been organized by platform and year to reveal patterns, trends, and comparative insights.

- **Overview of Social Media-Based Cybercrime Trends (2018–2023)**

The data shows a steady **year-on-year increase** in reported cybercrime cases involving major social media platforms. In 2018, the total number of reported cases stood at **6,500**, which rose to **11,750** by 2023 — indicating a near doubling of incidents over the six-year period. This sharp growth highlights the increasing vulnerability of social media users to cyber threats such as impersonation, financial fraud, cyberbullying, and data breaches.

Table 1: Year-Wise Social Media Cybercrime Cases (2018–2023)

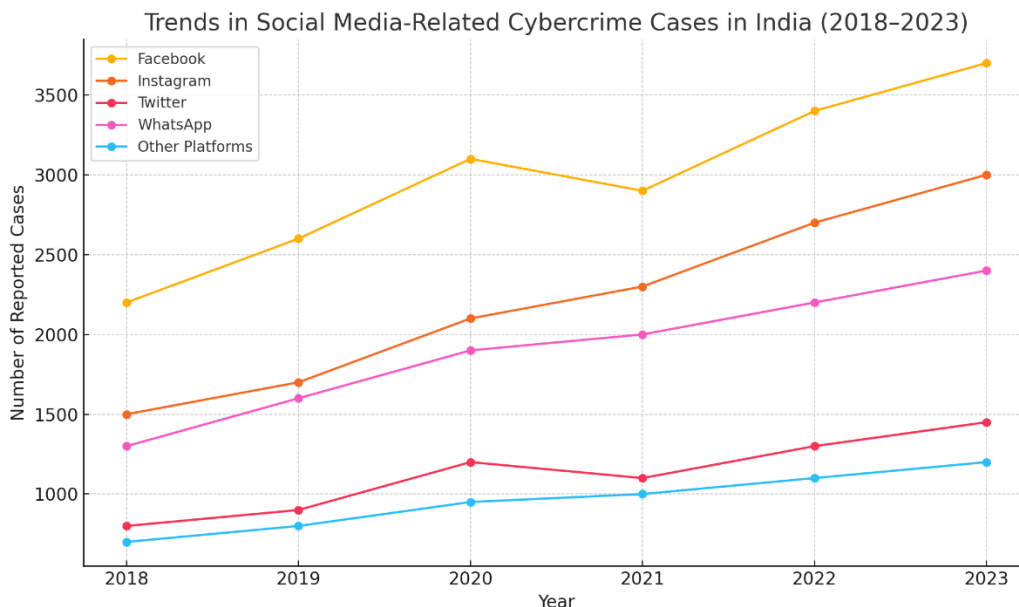
Year	Facebook	Instagram	Twitter	WhatsApp	Other Platforms	Total
2018	2200	1500	800	1300	700	6500
2019	2600	1700	900	1600	800	7600
2020	3100	2100	1200	1900	950	9250
2021	2900	2300	1100	2000	1000	9300

2022	3400	2700	1300	2200	1100	10700
2023	3700	3000	1450	2400	1200	11750

• Platform-Wise Analysis

Among the platforms, **Facebook** consistently recorded the highest number of cybercrime cases, rising from 2,200 in 2018 to 3,700 in 2023. This may be attributed to its large user base, extensive communication features, and susceptibility to impersonation or phishing attacks. **Instagram** also showed a sharp increase, from 1,500 cases in 2018 to 3,000 in 2023, reflecting its growing popularity, especially among younger demographics.

Figure 1: Platform-Wise Analysis

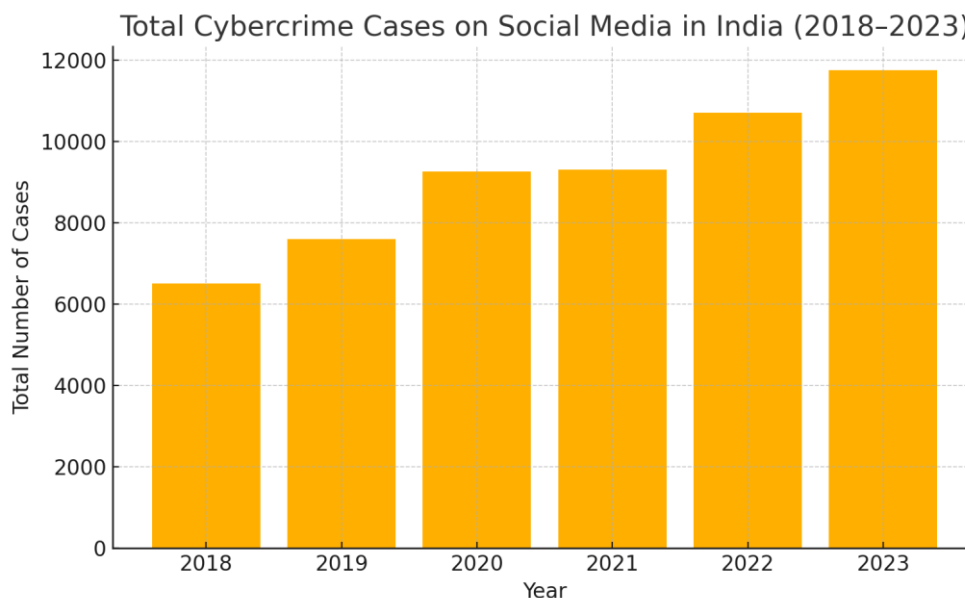


WhatsApp exhibited a moderate but steady increase in cases, rising from 1,300 in 2018 to 2,400 in 2023. The platform's encrypted nature often complicates detection and investigation of crimes such as fake news, financial scams, and harassment. **Twitter** (now X) showed relatively lower but rising numbers, from 800 to 1,450 cases in the same period. **Other platforms**, including lesser-known apps or community-based platforms, rose gradually, indicating that threats are expanding beyond mainstream services.

• Year-Wise Growth Analysis

The line chart representing platform-wise growth clearly shows **upward trends across all platforms**, with spikes during 2020 and 2021. These years coincide with the COVID-19 pandemic, during which internet and social media usage surged dramatically. The bar chart displaying **total annual cases** reinforces this trend, with notable jumps in 2020 and continued growth through 2023.

Figure 2: Year-Wise Growth Analysis



This increase reflects both the **rise in digital adoption** and possibly **improved awareness and reporting mechanisms**. However, it also underlines the evolving tactics of cybercriminals and the challenges in curbing such incidents.

• Comparative Insights Across Platforms

Comparative analysis across platforms reveals that **Facebook and Instagram** together account for over 50% of total reported cybercrime cases. While Facebook's long-standing presence contributes to its figures, Instagram's visual format and high youth engagement make it a new target for cybercriminal activity. The growing numbers on WhatsApp and Twitter suggest that messaging and microblogging platforms are equally at risk. This distribution calls for **platform-specific cybersecurity strategies** and stronger content moderation policies. It also suggests that users on visual or messaging platforms may be more vulnerable to fraud and psychological manipulation, including grooming, blackmail, and fake identities.

Conclusion

This study has drawn attention to the alarming rise of cybercrimes on social media platforms in India, analyzing both the technical patterns and the legal responses from 2018 to 2023. The evidence is clear: cybercrime incidents are increasing steadily, with platforms like Facebook and Instagram consistently leading in the number of reported cases. WhatsApp and Twitter also reflect a growing trend, reinforcing the fact that no platform is immune to misuse. The data demonstrates that the problem is not just expanding in volume but also evolving in complexity. While the Information Technology Act, 2000, and provisions of the Indian Penal Code offer a foundational legal structure, these measures are often reactive rather than preventive. Legal enforcement struggles to keep pace with the rapidly changing nature of digital platforms and cyber offenses.

The findings point to a pressing need for coordinated action. India must invest in strengthening cybercrime cells, enhancing technical infrastructure, and modernizing laws specific to digital and social media spaces. Equally important is platform-level responsibility and user education to reduce vulnerability.

References

1. A.J.W. Turner, *Kenny's Outlines of Criminal Law* (Cambridge University Press, U.K., 1st edn., 1962).
2. Albert J. Marcellai and Robert S. Greenfield, *Cyber Forensics: A Field Manual for Collecting, Examining and Processing Evidence of Computer Crime* (Auerbach Publications, London, 2002).
3. Amita Verma, *Cyber Crimes & Law* (Central Law House Publications, Allahabad, 1st edn., 2009).
4. Anirudh Rastogi, *Cyber Law – Law of Information Technology and Internet* (LexisNexis, Reed Elsevier India Pvt. Ltd., Gurgaon, 1st edn., 2014).
5. Austin, *Lectures on Jurisprudence: The Philosophy of Positive Law* (J. Murray, London, 1st edn., 1920).
6. Bary C. Collin, *The Future of Cyber Terrorism* (University of Illinois, Chicago, 1996).
7. C. Gringras, *The Laws of Internet* (Butterworth, U.K., 1997).
8. Chris Reed and John Angel, *Computer Law* (Oxford University Press, U.K., 3rd edn., 2003).
9. D. Thomas and B.D. Loader, *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age* (Routledge).
10. David Bainbridge, *Introduction to Computer Law* (Financial Time Management, 4th edn., 2000).

11. David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity Press, Cambridge, U.K., 2007).
12. Dorothy Denning, *Activism, Hacktivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy* (AMC Press, New York, 2001).
13. D.S. Yadav, *Foundation of Information Technology* (New Age International Publication Ltd., 3rd edn., 2007).
14. Edwin H. Sutherland, *Principles of Criminology* (Chicago Lippincott, 1947, 1965).
15. National Crime Records Bureau (NCRB), *Crime in India Reports (2018–2023)*, Ministry of Home Affairs, Government of India. Available at: <https://ncrb.gov.in>