

INTERNATIONAL JOURNAL OF LAW
MANAGEMENT & HUMANITIES
[ISSN 2581-5369]

Volume 9 | Issue 4

2026

© 2026 International Journal of Law Management & Humanities

Follow this and additional works at: <https://www.ijlmh.com/>

Under the aegis of VidhiAagaz – Inking Your Brain (<https://www.vidhiaagaz.com/>)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of any suggestions or complaints, kindly contact support@vidhiaagaz.com.

To submit your Manuscript for Publication in the International Journal of Law Management & Humanities, kindly email your Manuscript to submission@ijlmh.com.

Cybercrime and the Indian Legal System: An Analytical Approach

REBA SIBY*

ABSTRACT

Cybercrime has emerged as one of the most significant challenges in the era of rapid digitalisation. It is the duty of the authorities and of responsible citizens to meet this challenge with a strong legal framework. The rise in cybercrime is alarming because, unlike traditional crime, it is not easy to identify and punish offenders. The battlefield is highly technology-oriented, and those who master the technology hold power over this space. The digital divide that persists in society leaves many people helpless in confronting such crime, which makes a robust legal framework essential. In Indian conditions there is a very large population of internet users, but the majority of them lack a deep understanding of how technology operates, and this divide should make the government more thoughtful about securing them. The Information Technology Act, 2000, is the primary cyber-law of India, and it penalises cyber offences according to their gravity. The investigation of cybercrime is challenging, and the question of jurisdiction is one such difficulty, because these crimes take place on the internet and the offender may belong to any nation, so enforcement officers cannot exercise full authority without proper international cooperation. This article explores the multi-faceted nature of India's cybercrime framework and examines the strengths and weaknesses of the existing regime, arguing that this framework must be further secured.

Keywords: *cybercrime investigation, digital forensics, cyber law, technology, cybersecurity*

I. INTRODUCTION

The increase in cybercrime in India is an important concern, compounded by rapid digital growth and increasing internet availability. With over 700 million people accessing the internet, India has become a hotspot for cybercriminals (Basuroy, 2024). Cybercrimes ranging from financial fraud to identity theft affect internet users badly. Phishing scams are accompanied by more sophisticated attacks such as ransomware, spyware, and data breaches. The lack of cybersecurity awareness among users and weak legal frameworks aggravate the issue (Reddy, 2021).

* Author is an Assistant Professor at ABBS School of Law, Bengaluru, Karnataka, India.

One key factor behind the rise of cybercrime is the growth of digital payment systems and e-commerce platforms. While these developments have revolutionised convenience, they have also created new vulnerabilities. Cybercriminals exploit these weaknesses, often targeting naive individuals and businesses. In addition, the anonymity provided by the internet emboldens perpetrators, making it difficult to trace and punish them.

The impact of cybercrime is deep, affecting individuals, professionals, businesses, and even national safety. Financial loss, reputational damage, and mental-health harm are common after-effects for victims (Sharma, 2024). For businesses, cybercrime can halt operations and cause significant financial loss. On a larger scale, cybercrime poses a threat to critical infrastructure and national security (Kawoosa, 2024).

To counter this growing threat, India must improve its cybersecurity infrastructure, strengthen its legal frameworks, and promote awareness of cybersecurity among users. Joint efforts between the government, the private sector, and international bodies are important to address this issue effectively.

II. LEGAL FRAMEWORK OF THE INFORMATION TECHNOLOGY ACT, 2000

The Information Technology (IT) Act, 2000, is a key piece of legislation in India that addresses the challenges created by the digital era (Information Technology Act, 2000). Enacted to provide legal recognition to electronic transactions and digital signatures, the Act supports e-governance and seeks to secure online operations. It also defines several cybercrimes and prescribes penalties for offences such as hacking, identity theft, and data breaches (Athawale, 2021).

One of the Act's key features is its extensive jurisdiction, enabling it to address offences committed outside India where they involve a computer system located within India. The Act empowers the government to intercept communications and block access to websites under specified conditions, in the interest of national security and public order. However, certain provisions, such as Section 66A, were criticised for their potential for misuse and were subsequently struck down by the Supreme Court in 2015 in *Shreya Singhal v. Union of India* for violating the freedom of speech.

The IT Act has undergone amendments to address emerging issues, including data retention and privacy concerns. Despite its significance, the Act has been criticised for its vague provisions and enforcement difficulties, indicating the need for regular updates to keep pace with technological change (Prakash et al., 2023).

In sum, the IT Act, 2000, serves as the foundation of India's cyber-law framework, balancing the promotion of digital innovation with the need for regulation and security (Bhangla & Tuli, 2021). Its evolution reflects the dynamic nature of the digital ecosystem and the necessity of strong legal mechanisms to counter cyber threats.

III. STATUTORY PROVISIONS GOVERNING CYBERCRIMES IN INDIA

Cybercrime in India has risen rapidly with the spread of digitalisation, which calls for a section-wise analysis to understand its depth and dimensions (Vithalani, 2023). Cybercrime itself now includes several branches of differing gravity, and these should attract different punishments accordingly. The Information Technology (IT) Act, 2000, is the primary statute addressing cybercrime in India (Information Technology Act, 2000). Key provisions include Section 66, which deals with computer-related offences, and Section 67, which addresses the publication of obscene material in electronic form. In addition, Section 43 imposes a penalty for unauthorised access to computers, while Section 72 protects data privacy by penalising breaches of confidentiality.

The Bharatiya Nyaya Sanhita, 2023 (BNS) works alongside the IT Act (Bharatiya Nyaya Sanhita, 2023). For example, Section 318 deals with cheating, including online fraud, and Section 336 addresses forgery, including the forgery of digital documents. Cyber-stalking and harassment, particularly gender-based offences against women, are dealt with under Section 78 of the BNS.

Apart from these statutory provisions, challenges remain because of the ever-evolving nature of cybercrime. The lack of digital literacy among citizens and the limited cyber knowledge of law-enforcement agencies compound the problem. Recent studies point to the need for strong cybersecurity policies and public-awareness campaigns to reduce risks (Singh, 2023).

IV. PUNISHMENTS AND PENALTIES FOR CYBERCRIME OFFENCES

Punishments for cybercrime in India are governed by the Information Technology Act, 2000, and by important provisions of the Bharatiya Nyaya Sanhita, 2023 (BNS) (Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023). These laws address offences such as hacking, phishing, financial fraud, cyber-stalking, the use of trojan horses, and cyber-terrorism. The IT Act provides clear penalties for various cybercrimes. For instance, Section 66 penalises hacking with imprisonment of up to three years and/or a fine of up to five lakh rupees. Section 66C addresses identity theft, carrying imprisonment of up to three years and/or a fine of up to ₹1 lakh. Cyber-terrorism, under Section 66F, carries the most severe punishment, which may extend to imprisonment for life.

The BNS complements the IT Act by addressing issues such as defamation and the spreading of obscene content in cyberspace. Section 67 of the IT Act penalises the publication of obscene material online, with imprisonment of up to five years and a fine of up to ₹10 lakh for repeat offenders.

Despite these strict laws, enforcement remains a challenge because of the changing nature of cyber threats. Awareness programmes and cybersecurity measures are important in minimising risks and ensuring compliance.

V. BHARATIYA NYAYA SANHITA IN CYBERCRIME PROSECUTION

The Bharatiya Nyaya Sanhita, 2023 (BNS) plays a key role in the punishment of cybercrime in India, working alongside the Information Technology (IT) Act, 2000 (Bharatiya Nyaya Sanhita, 2023). While the IT Act is tailored to address cyber offences, the BNS provides a broad legal framework for setting punishments and penalties for crimes that involve conventional criminal elements, even when they occur in cyberspace (Deb, 2023).

For example, Section 336 of the BNS, which deals with forgery, is often used in cases of digital-document alteration and the tampering of electronic records. Similarly, Section 318(4), on cheating and dishonestly inducing the delivery of property, applies in cases of cyber fraud. Cyber-stalking, an increasing concern, is addressed under Section 78, which establishes the criminal nature of stalking in both conventional and digital spaces. Section 356, which deals with defamation, is also important for cases involving online abuse or false accusations.

The BNS ensures that cybercriminals are held accountable for offences that extend beyond the scope of the IT Act. This combined use of laws strengthens India's legal position against cybercrime (Sharma, 2022). However, challenges remain, such as issues of jurisdictional administration and the need for technical training for law-enforcement agencies (Gupta, 2021).

The balance between the BNS and the IT Act underlines the importance of a comprehensive legal approach to the multidimensional nature of cybercrime. As technology changes, so too must the interpretation and application of these laws, in order to ensure justice in the digital age.

VI. CHALLENGES IN ADDRESSING CYBERCRIME

Investigating cybercrime in India presents unique problems because of the rapid evolution of technology and the complex nature of cyber offences (Boruah, 2020). One key challenge is the lack of technical knowledge among law-enforcement agencies. Many officers are not adequately equipped to handle complicated cybercrimes, which frequently involve advanced and anonymous methods. In addition, jurisdictional issues arise, especially in cases involving

cross-border cybercrime, where international cooperation is often absent. The lack of a robust legal framework to address growing cyber threats further complicates investigations.

Another issue is the low rate of reporting of cybercrime. Victims often lack the confidence or the initiative to report incidents, owing to a lack of awareness or a fear of reputational harm. This under-reporting prevents the collection of the data needed to formulate sound policies and strategies.

Several measures can address these problems. First, improving the technical capabilities of law-enforcement agencies through proper training programmes is necessary. Developing a dedicated cybercrime unit equipped with advanced tools can significantly improve investigative efficiency. Second, pursuing international support through agreements and treaties can help address cross-border issues. Third, public-awareness campaigns would encourage victims to report cybercrime, ensuring better data gathering and use (Singh, 2023).

India's Information Technology Act, 2000, provides a legal system for confronting cybercrime, but it requires continuous updates to keep pace with technological advances. By adopting these measures, India can strengthen its cybercrime-investigation system and ensure a safer digital environment.

VII. DATA PROTECTION AND PRIVACY

Data protection and privacy in India have gained significant importance in recent years, especially with the spread of digitalisation across every sector and the increasing reliance on data-driven systems. The Supreme Court of India held that privacy is a fundamental right in the landmark case of *Justice K.S. Puttaswamy v. Union of India* (2017). This decision underlined the need for a strong legal system to safeguard personal data.

The Digital Personal Data Protection Act, 2023 (DPDP Act), is a crucial step in this direction (Digital Personal Data Protection Act, 2023). It sets out principles such as consent-based data use, purpose limitation, and accountability, while granting individuals rights such as notice, correction, and the right to erasure of information. The Act requires organisations to implement reasonable security safeguards to protect sensitive personal data. However, critics argue that the DPDP Act falls short in its enforcement mechanism and overall coverage compared with international standards such as the GDPR (General Data Protection Regulation) (Sharma & Gupta, 2023; Singh & Verma, 2024).

India's data-protection regime also includes the Information Technology Act, 2000, and its associated rules, which address cybersecurity and data breaches. Despite these steps, challenges

persist, including a lack of awareness, inadequate resources for enforcement, and the rapid growth of technology.

The interplay between the right to privacy and the right to access information remains a key area of focus. Striking a balance between protecting individual rights and enabling technological advancement is essential for India's digital development.

VIII. INTERNATIONAL COOPERATION IN CYBERCRIME LAW

International cooperation in tackling cybercrime is important because of the borderless nature of these offences. Cybercriminals exploit jurisdictional gaps, making cooperation between nations essential for effective prevention, investigation, and prosecution (Singh & Sharma, 2025). The Budapest Convention on Cybercrime, a landmark treaty, provides a basis for international cooperation, mutual assistance, and the preservation of data. In addition, the United Nations Convention against Cybercrime, adopted in 2024, seeks to strengthen global efforts to combat cybercrime and to facilitate the sharing of electronic evidence.

India has been consistently active in developing international cooperation to confront cybercrime (Gupta, 2025). The Indian Cybercrime Coordination Centre (I4C) functions as a nodal agency for coordinating action against cyber threats. India participates in global forums such as Interpol and the United Nations, contributing to knowledge-sharing and capacity-building. Legal reforms, including the Digital Personal Data Protection Act, align India's cybersecurity policies with international standards. India has also entered into bilateral agreements with several nations to enhance collaboration in cybercrime investigations.

India's efforts also include regional initiatives, such as the Shanghai Cooperation Organisation's cybersecurity framework. The government focuses on capacity-building by training law-enforcement officers and judicial staff. Public-awareness programmes and technical improvements further strengthen India's cybersecurity infrastructure. These efforts reflect India's commitment to developing international cooperation and ensuring a secure cyberspace.

IX. CYBERCRIME REPORTING AND INCIDENT RESPONSE

The reporting of cybercrime cases and incidents in India has improved significantly, reflecting the nation's commitment to countering the growing danger of cybercrime (Sharma & Gupta, 2023). The National Cybercrime Reporting Portal (NCRP), set up under the Indian Cybercrime Coordination Centre (I4C), serves as a centralised platform for people to report cybercrimes, including financial fraud and online defamation. This portal enables real-time tracking of cases and connects with law-enforcement bodies to ensure appropriate action. In addition, the

Indian Computer Emergency Response Team (CERT-In) plays an important role in incident response by issuing warnings, coordinating responses, and developing best practices (Kumar & Singh, 2024).

Despite these developments, challenges remain. Limited awareness among citizens about the reporting system, and the technical knowledge required for systematic incident response, reduce the system's efficiency. In addition, the lack of uniform protocols across states creates difficulties in handling cyber incidents.

To address these issues, India has created capacity-building programmes and public-awareness campaigns. The use of artificial intelligence and machine learning in cybercrime detection and response is also being explored to enhance efficiency. Collaboration with international bodies further develops India's ability to respond to cross-border cyber threats.

Although India has made significant progress in cybercrime detection and incident response, continued work on technology adoption, public awareness, and policy standardisation is important to build a resilient cybersecurity framework.

X. CONCLUSION AND RECOMMENDATIONS

India's cyber-law regime, driven by the Information Technology Act, 2000, has been instrumental in confronting cybercrime and promoting the digital ecosystem. However, the rapid advancement of technology demands a more robust and flexible legal framework to handle emerging challenges.

One key recommendation is the constant revision of relevant laws to address new-age cyber threats such as ransomware, phishing, and advanced persistent threats. The Digital Personal Data Protection Act, 2023, is a step forward, but its implementation must strike a balance between individual safety and national security. Improving global collaboration is also important for combating cybercrime; India should consistently engage in international cybersecurity agreements and programmes to improve its position on the world stage (Shaikh & Srivastava, 2025).

Promoting cyber literacy is another crucial aspect. Awareness programmes and training activities can help citizens and organisations adopt better cybersecurity practices. Establishing dedicated cybercrime courts and improving the capacity of law-enforcement agencies can aid the resolution of cybercrime cases and ensure that justice is served properly (Prakash et al., 2023).

Public-private cooperation can also play a key role in improving India's cyber-law framework. Collaboration between government bodies, academic institutions, and the private sector can drive innovation in cybersecurity technologies and policies.

By implementing these recommendations, India can develop a cyber-law framework that not only addresses current challenges but also anticipates future threats, ensuring a secure digital environment for its citizens.

XI. REFERENCES

- Athawale, A. P. (2021). Information Technology Act, 2000: An introduction of cyber-security provisions in India. *International Journal of Law*, 7(1), 26–29.
- Basuroy, T. (2024). Cybercrime in India: Statistics and trends. *Statista*, 15(4), 89–102.
- Bharatiya Nyaya Sanhita, No. 45 of 2023, Acts of Parliament, 2023 (India).
- Bhangla, A., & Tuli, J. (2021). A study on cybercrime and its legal framework in India. *International Journal of Law Management & Humanities*, 4(2), 493–504.
- Boruah, J. (2020). Cyber crimes and its legal challenges in India. *The Journal of Legal Methodology Policy and Governance*, 2(1).
- Deb, S. (2023). Cybercrime and the Indian Penal Code: A legal analysis. *Journal of Cyber Law Studies*, 15(2), 45–60.
- Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India).
- Gupta, A. (2021). Prosecution challenges in cybercrime cases under the IPC. *Cyber Law Review*, 8(1), 25–40.
- Gupta, A. (2025). India's role in global cybersecurity efforts. *International Journal of Cybersecurity*, 18(2), 89–102.
- Information Technology Act, No. 21 of 2000, Acts of Parliament, 2000 (India).
- Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.
- Kawoosa, A. (2024). Strengthening India's defence: Assessing legal frameworks for cyber-warfare preparedness. *Burnished Law Journal*.
- Kumar, S., & Singh, A. (2024). Incident response frameworks in India: A critical review. *International Journal of Cyber Law*, 12(2), 78–92.
- Prakash, P., Girdhar, S., & Jose, A. (2023). Indian cyber Act: Lacunae and recommendations. *International Journal of Law Management & Humanities*, 6(6), 2944–2954.

- Reddy, S. (2021). *Analytical study on cyber crimes in India*. SSRN.
- Shaikh, S. R., & Srivastava, A. (2025). Cyber law and digital privacy in India: A comprehensive analysis of legal frameworks, challenges, and future directions. *Lawful Legal Journal*.
- Sharma, R. (2022). The intersection of traditional and cyber laws in India. *Indian Journal of Legal Studies*, 10(3), 112–130.
- Sharma, R., & Gupta, A. (2023). Data protection laws in India: A critical analysis. *Journal of Cyber Law and Policy*, 15(2), 45–67.
- Sharma, R., & Gupta, P. (2023). Cybercrime reporting in India: Challenges and opportunities. *Journal of Cybersecurity Studies*, 15(3), 45–60.
- Sharma, T. (2024). The rise of cybercrimes in India and their impact on victims. *Indian Journal of Law and Legal Research*.
- Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
- Singh, G. (2023). Cybercrime in India: Trends, challenges, and mitigation strategies. *International Journal of Law, Policy and Social Review*, 5(3), 95–99.
- Singh, P., & Verma, S. (2024). Privacy in the digital age: Challenges and opportunities in India. *Indian Journal of Legal Studies*, 12(1), 89–102.
- Singh, R., & Sharma, P. (2025). Cybersecurity challenges and international cooperation: An Indian perspective. *Journal of Cyber Law and Policy*, 12(3), 45–60.
- Vithalani, N. P. (2023). Cybercrimes and law in India: A critical analysis. *International Journal of Creative Research Thoughts*, 11(8), 532–540.
