© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1717098

# Cybercrime under the IT Act, 2000 After the New Criminal Laws: Overlaps, Conflicts, and Gaps in Protection Against Online Harms

HARI NAGAICH[1], DR. TARU MISHRA[2]
[1,2]*Amity law School (Amity University Lucknow Campus)*

***Abstract-*** ***The rapid expansion of digital technologies has transformed social, economic, and political interactions across the world. India, with one of the fastest-growing digital economies, has experienced a significant rise in cybercrime alongside the expansion of internet connectivity and digital services. The Information Technology Act, 2000 (IT Act) represented India's first comprehensive legislative framework designed to regulate cyberspace and address cyber offences. However, technological evolution and the increasing sophistication of online harms have challenged the adequacy of this statute. The enactment of new criminal laws, particularly the Bharatiya Nyaya Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023, has reshaped India's criminal law landscape and introduced provisions that interact with the IT Act in complex ways. This paper examines the overlaps, conflicts, and gaps between the IT Act, 2000 and the new criminal laws in addressing cybercrime. It analyzes how similar conduct may fall under multiple statutory provisions, raising issues of legal interpretation, enforcement challenges, and potential double jeopardy concerns. The paper also highlights emerging threats such as deepfakes, large-scale data breaches, and cyberbullying that remain inadequately addressed within the current framework. Finally, it offers a critical perspective on the need for legislative harmonization, institutional capacity building, and the development of a modernized cyber law regime capable of responding to evolving digital threats.***

## I. INTRODUCTION

The digital revolution has fundamentally reshaped the nature of human interaction, commerce, governance, and communication. In India, the growth of internet penetration, digital payment systems, and e-governance initiatives has accelerated the country's transformation into a digitally driven society. Government programs such as Digital India, the widespread adoption of smartphones, and the increasing reliance on online platforms have created unprecedented opportunities for economic growth and social connectivity. However, these developments have also introduced new vulnerabilities and avenues for criminal activity.

Cybercrime today encompasses a wide range of illegal activities carried out using digital technologies. These include hacking, identity theft, online fraud, cyberstalking, dissemination of obscene or harmful content, ransomware attacks, and various forms of online harassment. Unlike traditional crimes, cyber offences often transcend geographical boundaries and can be executed anonymously, making detection and enforcement particularly challenging.

Recognizing the need for legal regulation of digital activities, the Indian Parliament enacted the Information Technology Act, 2000, which provided a legal framework for electronic transactions, digital signatures, and cybercrime offences. The Act was later amended in 2008 to incorporate additional provisions addressing emerging cyber threats, including identity theft and cyber terrorism.

Despite these reforms, technological developments have outpaced legislative responses. The increasing complexity of cybercrime has necessitated broader reforms within India's criminal justice system. In 2023, the government introduced a set of new criminal statutes replacing colonial-era laws, including the Bharatiya Nyaya Sanhita, 2023 (BNS), which replaced the Indian Penal Code; the Bharatiya Sakshya Adhiniyam, 2023, which replaced the Indian Evidence Act; and the Bharatiya Nagarik Suraksha Sanhita, 2023, which replaced the Code of Criminal Procedure.

While these new laws modernize several aspects of criminal law, they also create significant areas of interaction with the IT Act. Many cyber-related offences are now addressed both under the IT Act and the new criminal statutes. This overlap raises questions regarding the interpretation of statutory provisions, the applicability of the doctrine of special versus general laws, and the possibility of conflicting enforcement practices.

This paper seeks to explore these issues in depth. It examines the historical development of India's cybercrime laws, analyzes the intersections between the IT Act and the new criminal statutes, and evaluates the adequacy of existing legal mechanisms in addressing modern online harms. Through this analysis, the paper argues that while the introduction of new criminal laws represents a step toward modernization, the lack of harmonization between different legal frameworks continues to create uncertainty and enforcement challenges.

## II. LEGISLATIVE BACKGROUND

### Evolution of Cyber Law in India

India's cyber law regime developed in response to the growing need for legal recognition of electronic commerce and digital communication. Prior to the enactment of the IT Act, there was no comprehensive legal framework addressing electronic transactions or cyber offences. Traditional criminal laws were often inadequate to address crimes committed in digital environments.

The IT Act, 2000 was enacted primarily to give legal recognition to electronic records and digital signatures in accordance with the UNCITRAL Model Law on Electronic Commerce. However, the Act also introduced several provisions aimed at preventing misuse of computer systems and digital networks. These provisions established penalties for unauthorized access, data theft, hacking, and other cyber offences.

The Information Technology (Amendment) Act, 2008 significantly expanded the scope of cybercrime regulation. It introduced new offences such as identity theft, cheating by personation using computer resources, and cyber terrorism. The amendment also strengthened provisions relating to intermediary liability and data protection.

Despite these developments, critics have argued that the IT Act has several limitations. Many provisions remain vague, penalties are sometimes inadequate, and enforcement mechanisms have struggled to keep pace with technological advancements. In addition, the Act focuses primarily on individual offences rather than broader systemic threats such as large-scale data breaches or artificial intelligence-driven manipulation.

### Introduction of the New Criminal Laws

The enactment of the Bharatiya Nyaya Sanhita, 2023 (BNS) marks one of the most significant reforms in India's criminal law framework since independence. The BNS replaces the Indian Penal Code and introduces several provisions addressing contemporary forms of criminal behavior, including cyber-enabled offences.

Similarly, the Bharatiya Sakshya Adhiniyam, 2023 modernizes the rules of evidence by explicitly recognizing electronic records and digital evidence. This change is particularly significant in cybercrime cases, where digital trails often constitute the primary form of evidence.

However, these reforms have also created areas of overlap with the IT Act. Many cyber offences that were previously addressed exclusively under the IT Act can now also be prosecuted under the BNS. This dual applicability raises questions regarding jurisdiction, prosecutorial discretion, and the hierarchy of legal provisions.

## III. KEY PROVISIONS UNDER THE IT ACT, 2000

The IT Act contains several provisions addressing cyber offences and digital misconduct. Some of the most important sections are discussed below.

### Section 43: Damage to Computer Systems

Section 43 imposes civil liability for unauthorized access, downloading of data, introduction of computer contaminants such as viruses, and disruption of computer systems. The provision

primarily focuses on compensating victims for damage caused to digital infrastructure.

Section 66: Computer-Related Offences
Section 66 criminalizes acts listed under Section 43 when they are committed dishonestly or fraudulently. This section effectively transforms civil wrongs into criminal offences when malicious intent is present.

Section 66C: Identity Theft
Identity theft has become one of the most common forms of cybercrime. Section 66C penalizes the fraudulent use of another person's electronic signature, password, or unique identification feature. The offence carries a punishment of imprisonment for up to three years and a fine.

Section 66D: Cheating by Personation
Section 66D targets online fraud where individuals impersonate others using computer resources. Examples include phishing scams, fraudulent online banking schemes, and fake social media profiles used to deceive victims.

Section 67: Publishing Obscene Content
Section 67 criminalizes the publication or transmission of obscene material in electronic form. Additional provisions, such as Sections 67A and 67B, deal with sexually explicit material and child pornography.

These provisions form the backbone of India's cybercrime legislation. However, their interaction with newly enacted criminal laws has introduced new interpretational challenges.

## IV. RELEVANT PROVISIONS UNDER THE NEW CRIMINAL LAWS

Cyber-Related Offences under the Bharatiya Nyaya Sanhita
The Bharatiya Nyaya Sanhita includes several provisions that may apply to cyber-related conduct. For instance, offences such as cheating, fraud, and impersonation traditionally addressed under the Indian Penal Code—now exist within the BNS framework but may also occur through digital means. Similarly, offences related to stalking, sexual harassment, and defamation may increasingly occur in online environments. The BNS therefore provides a broader criminal law framework capable of addressing cyber-enabled misconduct.

Electronic Evidence under the Bharatiya Sakshya Adhiniyam
The Bharatiya Sakshya Adhiniyam modernizes evidentiary rules by explicitly recognizing electronic records as admissible evidence. This is particularly relevant in cybercrime investigations, where digital logs, metadata, and electronic communications serve as key sources of proof.

The Act aims to simplify procedures for authentication of digital evidence while ensuring reliability and integrity. However, practical challenges remain in terms of digital forensics expertise and infrastructure.

## V. OVERLAPS BETWEEN THE IT ACT AND NEW CRIMINAL LAWS

The coexistence of the IT Act and the new criminal statutes have created several areas of overlap where the same conduct may fall under multiple legal provisions.

Identity Theft and Online Fraud
Identity theft and online fraud provide a clear example of overlapping provisions. Under the IT Act, such conduct may be prosecuted under Sections 66C and 66D. However, similar conduct may also constitute cheating or impersonation under the BNS.
This overlap raises questions about prosecutorial discretion and the appropriate statute under which charges should be framed. While the IT Act is a specialized law dealing specifically with cyber offences, the BNS provides broader criminal provisions applicable to both online and offline conduct.

Online Harassment and Stalking
Cyberstalking and online harassment often involve behaviors such as repeated messaging, surveillance through social media, or unauthorized monitoring of digital activities. While certain aspects of these behaviors may fall within the scope of the IT Act—particularly where computer systems are misused—

others may be prosecuted under stalking provisions in the BNS.

Obscenity and Sexual Content Online

The dissemination of obscene or sexually explicit material online can be prosecuted under Section 67 of the IT Act. However, the BNS also contains provisions addressing obscenity and harassment. This dual framework may lead to multiple charges for the same conduct.

From a legal perspective, such overlaps can complicate enforcement and create uncertainty regarding the application of the doctrine of double jeopardy, which prohibits an individual from being punished twice for the same offence.

## VI. CONFLICTS IN LEGAL FRAMEWORKS

Special Law vs General Law

One of the most significant legal questions arising from the coexistence of the IT Act and the new criminal laws concerns the relationship between special laws and general laws.

The IT Act is generally considered a special statute designed specifically to regulate cyber activities. According to established principles of statutory interpretation, a special law typically prevails over a general law when both apply to the same subject matter.

However, the new criminal statutes do not explicitly clarify whether their provisions are subordinate to or independent of the IT Act. This ambiguity may lead to conflicting judicial interpretations.

Differences in Punishment

In some cases, the IT Act and the BNS prescribe different penalties for similar conduct. For example, the punishment for cheating under the BNS may differ from the punishment for online impersonation under the IT Act. Such discrepancies may influence prosecutorial decisions and potentially lead to inconsistent sentencing outcomes.

Procedural Challenges

Cybercrime investigations often require specialized technical expertise, digital forensics capabilities, and cross-border cooperation. While the IT Act provides certain procedural powers to law enforcement agencies, the broader criminal procedure framework under the new laws may operate differently.

These differences can create confusion regarding investigative authority, jurisdiction, and admissibility of digital evidence.

## VII. GAPS IN PROTECTION AGAINST ONLINE HARMS

Despite the existence of overlapping legal provisions, significant gaps remain in India's cybercrime framework.

## VIII. DEEPFAKES AND ARTIFICIAL INTELLIGENCE

One of the most pressing challenges in the digital age is the rise of deepfake technology, which uses artificial intelligence to create realistic but fabricated images, videos, or audio recordings. Deepfakes can be used for political misinformation, financial fraud, or harassment.

Current laws do not specifically address the creation or distribution of malicious deepfakes. While existing provisions on defamation or obscenity may apply in certain cases, they are not tailored to the unique challenges posed by AI-generated content.

## IX. DATA BREACHES AND PRIVACY VIOLATIONS

Large-scale data breaches have become increasingly common, affecting millions of users. While certain provisions of the IT Act address unauthorized access to computer systems, they do not comprehensively regulate corporate responsibility for safeguarding user data.

India's evolving data protection framework may address some of these concerns, but enforcement mechanisms remain in development.

## X. CYBERBULLYING

Cyberbullying is a growing problem, particularly among young internet users. It involves repeated harassment, threats, or humiliation through digital

platforms. Although certain acts may fall under harassment or defamation laws, there is no specific provision addressing cyberbullying as a distinct offence.

## XI. MY OPINION

In my view, India's cyber law framework is at a critical stage of development. The IT Act, 2000 was undoubtedly a pioneering statute when it was enacted, providing the first legal recognition of cyber offences in the country. However, the pace of technological advancement over the past two decades has far exceeded the scope originally envisioned by the legislation.

The introduction of the new criminal laws represents an important attempt to modernize India's criminal justice system. Nevertheless, the coexistence of multiple overlapping legal frameworks may inadvertently create confusion for law enforcement agencies, prosecutors, and courts. Instead of providing clarity, duplication of provisions sometimes leads to uncertainty about which statute should be applied in a particular case.

From a policy perspective, a more coherent and unified approach to cybercrime regulation may be necessary. Rather than maintaining separate and partially overlapping statutes, lawmakers could consider developing a comprehensive cybercrime code that consolidates relevant provisions from the IT Act and the criminal statutes. Such a framework would improve clarity, streamline enforcement, and ensure that emerging digital threats are addressed more effectively.

Equally important is the need for institutional capacity building. Cybercrime investigations require specialized knowledge of digital systems, encryption technologies, and online platforms. Without adequate training and resources, law enforcement agencies may struggle to effectively implement even well-designed legal provisions.

Public awareness also plays a crucial role in combating cybercrime. Many victims of online fraud or harassment are unaware of available legal remedies or hesitate to report incidents due to stigma or lack of confidence in the justice system. Strengthening reporting mechanisms and promoting digital literacy could significantly enhance the effectiveness of cybercrime prevention strategies.

## XII. CONCLUSION

India's legal framework for addressing cybercrime has evolved significantly since the enactment of the IT Act in 2000. The introduction of new criminal statutes in 2023 marks a major step toward modernizing the country's criminal justice system. However, the interaction between these laws has created both opportunities and challenges.

Overlaps between the IT Act and the new criminal laws may provide multiple avenues for prosecution but also risk creating confusion and inconsistent enforcement. Conflicts regarding the hierarchy of legal provisions, differences in punishment, and procedural complexities further complicate the legal landscape.

At the same time, emerging technological threats including deepfakes, large-scale data breaches, and cyberbullying highlight the limitations of existing laws. Addressing these challenges will require a forward-looking legislative approach that balances innovation with effective regulation.
Ultimately, a harmonized and comprehensive cyber law framework, supported by strong institutional capacity and public awareness, will be essential to ensuring meaningful protection against online harms in the digital age.

## REFERENCES

[1] A. Tandon, "Double Jeopardy in Indian Cyber Law: IT Act and BNS Overlaps," Indian Journal of Law & Technology, Vol. 22, No. 1 (2024), pp. 34–47.

[2] R. Chatterjee, "Special or General? The Conflict of Laws in Indian Cybercrime Prosecution," National Law Review, Vol. 18, No. 2 (2024), pp. 55–69.

[3] Ministry of Electronics and Information Technology, Government of India, White

Paper on Emerging Cyber Threats and Legal Gaps (2023), pp. 12–16.

[4] Pavan Duggal, Cyberlaw: The Indian Perspective (LexisNexis, 2022).

[5] Apar Gupta, “Regulating Cyberspace in India: Challenges and Opportunities,” Journal of National Law University Delhi, Vol. 10 (2021).

[6] UNCITRAL Model Law on Electronic Commerce (1996).