INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 12 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

THE EVOLUTION OF MAJOR TYPES OF CYBERCRIME AND CRITICALLY ANALYZES THE EFFECTIVENESS OF THE INFORMATION TECHNOLOGY ACT, 2000 (IT ACT), AND OTHER SUBSEQUENT LEGAL AND INSTITUTIONAL FRAMEWORKS IN INDIA TO COMBAT THESE THREATS

AUTHOR - V R KALYANI, STUDENT AT VELS INSTITUTE OF SCIENCE, TECHNOLOGY AND ADVANCED STUDIES

BEST CITATION - V R KALYANI, THE EVOLUTION OF MAJOR TYPES OF CYBERCRIME AND CRITICALLY ANALYZES THE EFFECTIVENESS OF THE INFORMATION TECHNOLOGY ACT, 2000 (IT ACT), AND OTHER SUBSEQUENT LEGAL AND INSTITUTIONAL FRAMEWORKS IN INDIA TO COMBAT THESE THREATS, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 5 (12) OF 2025, PG. 1045-1050, APIS – 3920 – 0001 & ISSN - 2583-2344

Abstract

This research critically examines the dynamic landscape of cybercrime in India and assesses the efficacy of the Information Technology Act, 2000 (IT Act), alongside allied legal and institutional frameworks. The exponential rise in digital transactions, fueled by national digitalization initiatives, has simultaneously fueled a surge in sophisticated cyber threats, including financial fraud, Ransomware-as-a-Service (RaaS), and the misuse of emerging technologies like deepfakes.

The study employs a mixed-methods approach, combining doctrinal analysis of key statutes (the IT Act, the newly enacted Digital Personal Data Protection Act (DPDPA), 2023, and the Indian Evidence Act) with an empirical review of governmental data and judicial pronouncements.

The findings reveal that while the IT Act provided a foundational legal basis for digital governance and crime prosecution, it suffers from significant obsolescence and procedural challenges. Critically, the primary impediment to effective justice is not a lack of statutory definitions but the low conviction rate stemming from profound institutional weaknesses. These weaknesses include the rigorous and often impractical requirements of Section 65B of the Indian Evidence Act for digital evidence admissibility, the lack of sufficient digital forensics capacity within law enforcement, and persistent jurisdictional complexities in tackling cross-border crimes.

The introduction of the DPDPA, 2023, is recognized as a vital step towards enhancing data accountability, but its enforcement mechanism must be seamlessly integrated with the penal framework of the IT Act to avoid jurisdictional conflict. The research concludes that the existing legal structure remains a paper tiger unless immediate, targeted reforms are made to simplify evidence rules, dramatically enhance the technical capabilities of law enforcement, and mandate specialized training for the judiciary.

Keywords - Cybercrime, Information Technology Act, 2000, IT Act Effectiveness, Digital Evidence, Section 65B, Digital Personal Data Protection Act (DPDPA) 2023, Ransomware, Cyber Law India, Conviction Rate

Research Aim

To critically analyze the effectiveness of the Information Technology Act, 2000, and subsequent legal and institutional frameworks in India in addressing the contemporary landscape of major cybercrimes, and to

propose recommendations for legal and enforcement reform.

Need for the Research

The rapid and ubiquitous digitalization in India—encompassing e-commerce, digital governance, and financial transactions—has led to an exponential increase in both the volume and sophistication of cybercrimes.

Surging Cybercrime Rates: Official statistics from agencies like the National Crime Records Bureau (NCRB) and reports by organizations like CERT-In consistently indicate a sharp rise in reported cybercrime incidents, suggesting that existing legal and enforcement mechanisms may be insufficient to deter or prosecute effectively.

Technological Obsolescence: The core legislation, the IT Act, 2000, was enacted at a nascent stage of the internet. Despite amendments, its provisions may not fully address new forms of crime like Ransomware-as-a-Service (RaaS), advanced social engineering, and deepfakes.

Digital Economy Protection: A robust and effective legal framework is paramount for maintaining public trust and ensuring the security of India's multi-trillion-dollar digital economy and critical information infrastructure.

Jurisdictional and Evidentiary Challenges: Cybercrimes often transcend national boundaries, creating complex issues of jurisdiction, extradition, and the admissibility of digital evidence in court, which current laws and procedural practices may struggle to resolve efficiently.

Research Gap

While numerous studies have outlined the provisions of the IT Act and categorized cybercrimes, a significant gap exists in the empirical and critical evaluation of its on-ground effectiveness, particularly concerning:

Low Conviction Rate: There is a lack of comprehensive, up-to-date analysis linking specific sections of the IT Act to the success rates of prosecution (conviction vs. Acquittal) in major cybercrime cases.

Inter-Framework Cohesion: Limited research critically examines the interplay and potential conflicts between the IT Act, the newly introduced Digital Personal Data Protection Act (DPDPA), 2023, and traditional criminal laws like the Indian Penal Code (IPC) and the new Bharatiya Nyaya Sanhita (BNS) in prosecuting cyber offences.

Law Enforcement Capacity vs. Crime Sophistication: A shortage of research assesses the gap between the specialized training, forensic capabilities, and resource allocation to law enforcement agencies (LEAs) and the increasingly complex techniques used by transnational cybercriminals.

Research Issues

The research will focus on the following core issues:

Categorization of Cybercrimes: What are the most prevalent and emerging forms of cybercrime in India (e.g., financial fraud, identity theft, cyberstalking, ransomware, cyber-terrorism, and deepfake abuses), and how adequately are they defined and addressed under the existing legal framework?

Effectiveness of the IT Act, 2000: What are the major statutory and procedural lacunae in the IT Act and related frameworks that hinder effective investigation, prosecution, and adjudication of cybercrime cases?

Role of New Legislation: To what extent does the Digital Personal Data Protection Act, 2023, complement or complicate the enforcement efforts under the IT Act, 2000, particularly in cases involving data breaches and identity theft?

Enforcement and Institutional Challenges: What are the primary practical and institutional challenges faced by police, cyber cells, and the judiciary (e.g., digital forensics, jurisdictional complexity, and judicial technological literacy)

that contribute to the low rate of convictions in cybercrime cases?

Literature Review

The review draws on primary legislation, scholarly databases (HeinOnline, Google Scholar, Manupatra), and journalistic analysis.

Major Types of Cybercrime and Statutory Response

The literature confirms that cybercrimes have shifted from rudimentary hacking to sophisticated, financially motivated schemes. Phishing, Identity Theft, and Financial Fraud (often addressed under Sections 43, 66, and 66C/D of the IT Act, read with IPC/BNS sections like cheating) are reported as the most common. Scholarly articles emphasize that the IT Act has core provisions—like Section 66 (Hacking) and Section 67 (Obscenity)—that define basic offences, but they often lack the technical specificity required to prosecute modern malware and cloud-based attacks. Editorials often highlight the alarming rise of ransomware and sextortion, which exploit the anonymity of the internet, revealing a gap between legal definitions and criminal practice.

Critical Analysis of the IT Act, 2000

Academics generally view the IT Act, 2000, as a pioneering but increasingly outdated framework.

Initial Success: Studies acknowledge the Act's success in providing legal recognition to electronic records and digital signatures (Sections 4, 5, 10A), thereby facilitating e-commerce.

Substantive Deficiencies:

Research points to the vagueness of key terms and the inadequacy of penalties for severe offences. The landmark Supreme Court ruling in Shreya Singhal v. Union of India highlighted the legislative overreach and ambiguity, leading to the striking down of the controversial Section 66A.

Evidentiary Hurdles:

Scholarly research consistently flags Section 65B of the Indian Evidence Act (admissibility of electronic records) as a major procedural bottleneck, with strict technical requirements for certification often leading to the exclusion of crucial digital evidence.

Emerging Legal Frameworks and Institutional Response

Recent literature and government reports (PIB, NCRB) focus on the advent of the DPDPA, 2023. This law is hailed as a significant step toward consumer protection and data accountability, imposing stricter obligations on Data Fiduciaries and introducing substantial penalties for data breaches. However, articles in legal journals and leading English dailies debate its practical integration with the IT Act, noting potential jurisdictional overlaps between the proposed Data Protection Board and the existing IT Adjudicating Officers. Institutional efforts like the Indian Cybercrime Coordination Centre (I4C) and the dedicated helpline '1930' are recognized as positive steps toward centralized reporting and coordinated enforcement, though their effectiveness is still under scrutiny.

Research Methodology

This research will employ a mixed-methods approach involving both qualitative and quantitative legal analysis.

1. **Doctrinal Research (Qualitative)**

Statutory Analysis: A deep-dive study of the IT Act, 2000 (as amended), the DPDPA, 2023, relevant provisions of the Indian Evidence Act, 1872 (specifically Section 65B), and the Bharatiya Nyaya Sanhita (BNS).

Case Law Analysis: Examination of reported and landmark judgments from the Supreme Court and High Courts (using Manupatra, HeinOnline) concerning cybercrime prosecution under the IT Act to identify judicial interpretations, application of evidentiary rules, and reasons for acquittal/conviction.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 12 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

2. **Empirical Research (Quantitative and Qualitative)**

Data Collection: Analysis of publicly available, aggregated data from the NCRB and CERT-In regarding:

Trends in cybercrime types and victim demographics.

Comparison of the number of cases registered, cases chargesheeted, and cases convicted under the IT Act.

Comparative Institutional Review: A study of the mandates, coordination mechanisms, and resource allocation for key enforcement bodies: Cyber Cells, the I4C, and the CERT-In.

Literature Synthesis: Integration of scholarly articles and professional reports from Google Scholar and leading dailies to incorporate expert commentary and public awareness of the law's effectiveness.

Scheme of Lessons (Chapter Outline)

Chapter

Title

Focus Area

I

Introduction

Research context, aim, need, scope, research questions, and methodology.

II

Understanding Cybercrime: Typology and Evolution

Detailed categorization of major cybercrimes (e.g., Hacking, Malware/Ransomware, Phishing, Identity Theft, Cyber-terrorism) and their technological progression in the Indian context.

III

The Statutory Framework: IT Act, 2000 and Allied Laws

In-depth analysis of key penal provisions of the IT Act (Sections 43, 66, 66B-66F, 67, 72) and their intersection with the IPC/BNS and the role of the DPDPA, 2023.

IV

Critique of Legal Effectiveness: Judicial and Evidentiary Challenges

Critical analysis of case laws, focusing on conviction rates, judicial interpretation of 'computer resource' and 'data,' and the procedural complexities under Section 65B of the Indian Evidence Act.

V

Enforcement and Institutional Gaps

Assessment of the effectiveness of the I4C, Cyber Cells, digital forensics capacity, and challenges of international cooperation (jurisdiction and Mutual Legal Assistance Treaties).

VI

Research Report: Findings and Analysis

Presentation and analysis of empirical data on cybercrime trends and the conviction-to-registration ratio under the IT Act. Discussion of the gap between the law's intent and its execution.

VII

Conclusion and Recommendations

Summary of findings, conclusion on the effectiveness of the legal framework, and concrete recommendations for legislative and institutional reforms.

Research Report Based on the Issues

1. Categorization of Cybercrimes: Prevalent and Emerging Threats

The research confirms that while the IT Act adequately covers foundational offences like unauthorized access (Hacking – Sec. 66) and obscene material (Sec. 67), it struggles with the nuances of modern, highly profitable cybercrimes.

Financial Fraud: The majority of reported cases are variations of financial fraud, often prosecuted under both IT Act (e.g., Sec. 66D for cheating by personation) and the IPC/BNS (e.g., cheating). This dual-prosecution highlights the

IT Act's inability to exclusively handle many high-volume online financial crimes, requiring reliance on traditional laws.

Ransomware: This major threat, involving encrypted data and ransom demands, is generally shoehorned into the category of "damage to computer source code" (Sec. 66) or "cyber-terrorism" (Sec. 66F), which may not fully capture the nature and scale of the extortion involved, leading to less precise prosecution.

Deepfakes and Misinformation: Emerging crimes like the malicious use of AI-generated deepfakes for impersonation or defamation are inadequately addressed. They currently rely on broad sections like Sec. 66D or Sec. 67, lacking specific, deterrent provisions.

2. Effectiveness of the IT Act, 2000: Statutory and Procedural Lacunae

Empirical data (as consistently reflected in scholarly work referencing NCRB reports) suggests a critically low conviction rate for cybercrimes under the IT Act, which is a key indicator of its limited on-ground effectiveness.

Statutory Vagueness: The broad language used in key sections (e.g., the definition of 'data' or 'computer system') leads to varying judicial interpretations, creating unpredictability in legal outcomes.

Section 65B of the Indian Evidence Act: This section is a major bottleneck. Its strict pre-conditions for the certification of electronic records (such as server logs, CDRs, and intercepted communications) are often not met by investigators, leading to the exclusion of primary evidence. This single procedural flaw significantly contributes to acquittals, even in otherwise strong cases.

3. Role of New Legislation: Inter-Framework Challenges

The Digital Personal Data Protection Act (DPDPA), 2023, represents a shift toward a data governance model rather than just a penal one.

Positive Complement: The DPDPA enhances the framework by imposing strict compliance and accountability on data fiduciaries, thereby preventing data breaches that often fuel identity theft and financial crimes under the IT Act.

Challenges: Potential overlaps exist in enforcement. For instance, a data breach may trigger a significant fine under the DPDPA's Data Protection Board and also a criminal investigation under IT Act's Section 43A (negligence in protecting sensitive personal data) and/or Sec. 66 for unauthorized access. The lack of a clear, seamless coordination mechanism between the two regulatory and penal bodies can lead to administrative friction and potential double jeopardy issues.

4. Enforcement and Institutional Challenges

The gap between the complexity of cybercrime and the capacity of LEAs remains a critical finding, frequently highlighted in editorials from leading dailies.

Digital Forensic Capabilities: Many local cyber cells lack the necessary resources, trained personnel, and state-of-the-art forensic tools to effectively analyze encrypted devices, trace cryptocurrency transactions, and conduct cross-border investigations.

Jurisdiction: The transnational nature of cybercrime (e.g., servers located abroad, foreign perpetrators) complicates jurisdiction. Relying on slow-moving Mutual Legal Assistance Treaties (MLATs) hinders the rapid collection of evidence, which is crucial for volatile digital data.

Judicial Literacy: A lack of specialized training among the judiciary on technical concepts of digital evidence, blockchain, and network forensics often results in overly strict application of technical laws, favoring the accused and perpetuating the low conviction rate.

Research Conclusion Based on the Research Report

The Information Technology Act, 2000, along with its amendments, serves as a necessary but increasingly insufficient bedrock for combating modern cybercrime in India.

The research concludes that the primary hindrance to the effectiveness of the legal framework is not merely the absence of laws to categorize new crimes, but rather the procedural and institutional failings in their enforcement.

The low conviction rate is a clear indicator that the law fails to translate successful investigation into successful prosecution, a failure largely attributable to the stringent and poorly implemented technical requirements for digital evidence admissibility (Sec. 65B) and the limited technical capacity of law enforcement and the judiciary.

While the new DPDPA, 2023, is a progressive step towards data governance and accountability, its success in crime deterrence hinges on effective synergy with the penal framework of the IT Act and a clear demarcation of regulatory and criminal jurisdiction.

To effectively fight cybercrime, India needs not just new laws, but a fundamental overhaul of its institutional and procedural mechanisms—specifically, by simplifying digital evidence rules, investing significantly in specialized digital forensics, and institutionalizing mandatory, ongoing technological training for police and judicial officers. The current framework risks becoming a paper tiger, unable to effectively tackle the escalating digital menace.

Footnote

https://www.researchgate.net/publication/393383488_A_study_on_issues_and_challenges_of_information_technology_act_2000_in_India?hl=en-IN

https://indianexpress.com/about/cyber-crime/?hl=en-IN#:~:text=Another%20contributing%20factor%20is%20the,to%20track%20and%20prosecute%20offenders.

https://cleartax.in/s/it-act-2000?hl=en-IN

https://www.pib.gov.in/PressReleasePage.aspx?PRID=2176146&hl=en-IN#:~:text=Digital%20Personal%20Data%20Protection%20Act,and%20more%20accountable%20for%20everyone.

https://www.pib.gov.in/PressReleasePage.aspx?PRID=2176146&hl=en-IN#:~:text=Strengthening%20Law%20Enforcement%20Capacity,an%20organised%20and%20coordinated%20manner.