INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

CYBERCRIME AND DIGITAL EVIDENCE UNDER INDIAN LEGAL FRAMEWORK

AUTHORED BY - DR K RAMA KRISHNA BABA
Faculty, Dr B R Ambedkar Department of Legal Studies
Acharya Nagarjuna University, Guntur, Andhra Pradesh

ABSTRACT

India is confronting an unprecedented surge in cybercrime, with NCRB data revealing a 247% increase in registered cybercrime cases between 2018 and 2023, reaching 94,432 cases. This paper undertakes a comprehensive legal analysis of India's cybercrime framework under the Information Technology Act 2000 (as amended in 2008) and complementary provisions of the Indian Penal Code 1860, the Bharatiya Nyaya Sanhita 2023, and the Indian Evidence Act 1872. A central focus of the paper is the admissibility, authentication, and evidentiary value of digital evidence in Indian courts, an area characterised by inconsistent judicial interpretation, inadequate forensic standards, and rapidly evolving technological challenges including cloud computing, encrypted communications, and blockchain evidence. The paper critically examines landmark judicial decisions including Anvar P.V. v P.K. Basheer (2014), Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020), and Sonu v State of Haryana (2017) on the certification requirements for electronic evidence under Section 65B of the Indian Evidence Act. The study further analyses the investigative powers and procedural framework under the IT Act, jurisdictional challenges in cybercrime prosecution, the role of CERT-In, and India's obligations under the Budapest Convention on Cybercrime.

Keywords: *Cybercrime, Digital Evidence, Section 65B, IT Act 2000, CERT-In, Digital Forensics, Bharatiya Nyaya Sanhita 2023*

1. INTRODUCTION

Cybercrime has emerged as one of the most significant threats to India's social fabric, economic security, and national sovereignty in the digital age. Unlike conventional crime, which is geographically bounded and temporally discrete, cybercrime transcends physical boundaries, operates in real-time across multiple jurisdictions, exploits technical vulnerabilities in critical

 ISSN: 2582-6433

infrastructure, and leaves evidentiary traces that are simultaneously ubiquitous and fragile. The exponential growth of internet connectivity in India — from 250 million users in 2015 to over 900 million in 2024 — has dramatically expanded both the attack surface for cybercriminals and the potential victim population.

The Indian criminal justice system, built around the evidentiary paradigm of physical evidence and eyewitness testimony, has struggled to adapt to the challenges of digital investigation and prosecution. Digital evidence, by its very nature, is volatile (susceptible to alteration or deletion), technical (requiring specialised expertise to interpret), and legally contested (subject to challenges of authenticity, integrity, and admissibility). The intersection of these challenges with India's complex federal structure, overburdened criminal courts, and limited forensic infrastructure creates a 'justice gap' in cybercrime prosecution that emboldens perpetrators and leaves victims without adequate redress.

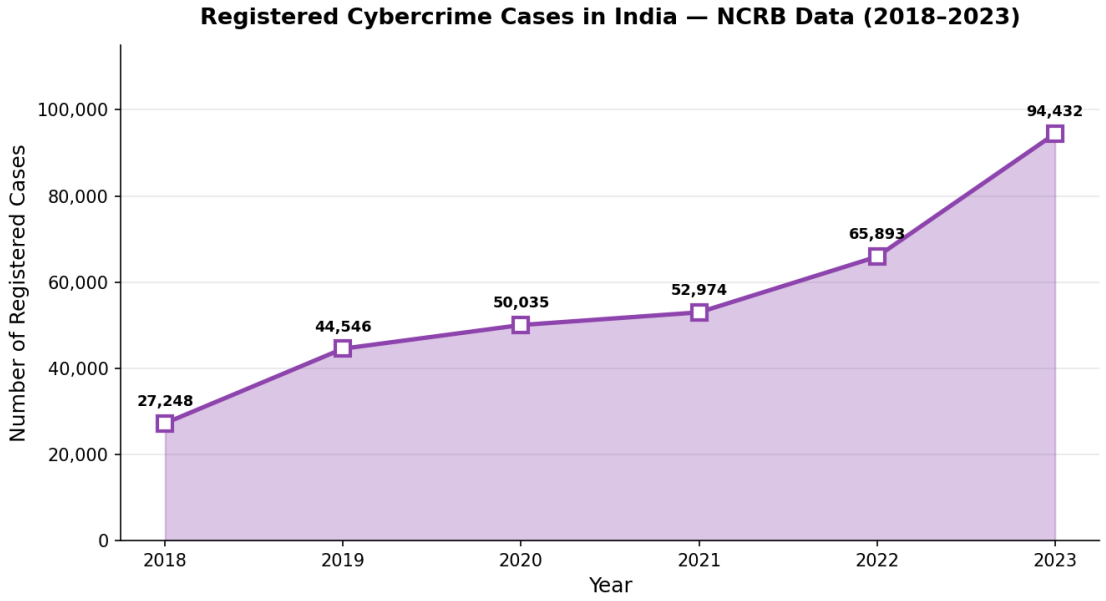

Figure 1: Registered Cybercrime Cases in India — NCRB Data (2018–2023) — Source: National Crime Records Bureau Annual Reports

1.1 Research Objectives

- To analyse the legislative architecture of the IT Act 2000 and its adequacy for addressing contemporary cybercrime.
- To critically examine the Section 65B digital evidence framework and its judicial evolution.
- To analyse specific categories of cybercrime and their legal treatment under Indian law.

ISSN: 2582-6433

- To identify gaps in investigative framework, forensic infrastructure, and international cooperation.
- To propose comprehensive legislative and institutional reforms for cybercrime governance in India.

2. THE INFORMATION TECHNOLOGY ACT 2000: ARCHITECTURE AND ANALYSIS

The Information Technology Act 2000, enacted on 17 October 2000 and significantly amended by the Information Technology (Amendment) Act 2008, provides the primary legislative framework for electronic governance, digital commerce, and cybercrime in India. The Act was enacted pursuant to Entry 31 of List I (Union List) and Entry 97 of the Seventh Schedule to the Constitution.

2.1 Key Offences Under the IT Act

- Section 43: Penalty and Compensation for damage to computer, computer system — civil liability for unauthorised access, damage, disruption, and data theft.
- Section 66: Computer Related Offences — criminalises dishonest or fraudulent acts involving computer systems, punishable with imprisonment up to 3 years and fine up to Rs.5 lakh.
- Section 66C: Identity Theft — fraudulent use of electronic signature, password or unique identification feature — imprisonment up to 3 years.
- Section 66D: Cheating by personation by using computer resource — imprisonment up to 3 years.
- Section 66E: Violation of Privacy — publishing private images — imprisonment up to 3 years or fine up to Rs.2 lakh.
- Section 66F: Cyber Terrorism — acts threatening national integrity, sovereignty or causing death through computer — punishment up to life imprisonment.
- Section 67: Publishing obscene material in electronic form — imprisonment up to 5 years.

 ISSN: 2582-6433

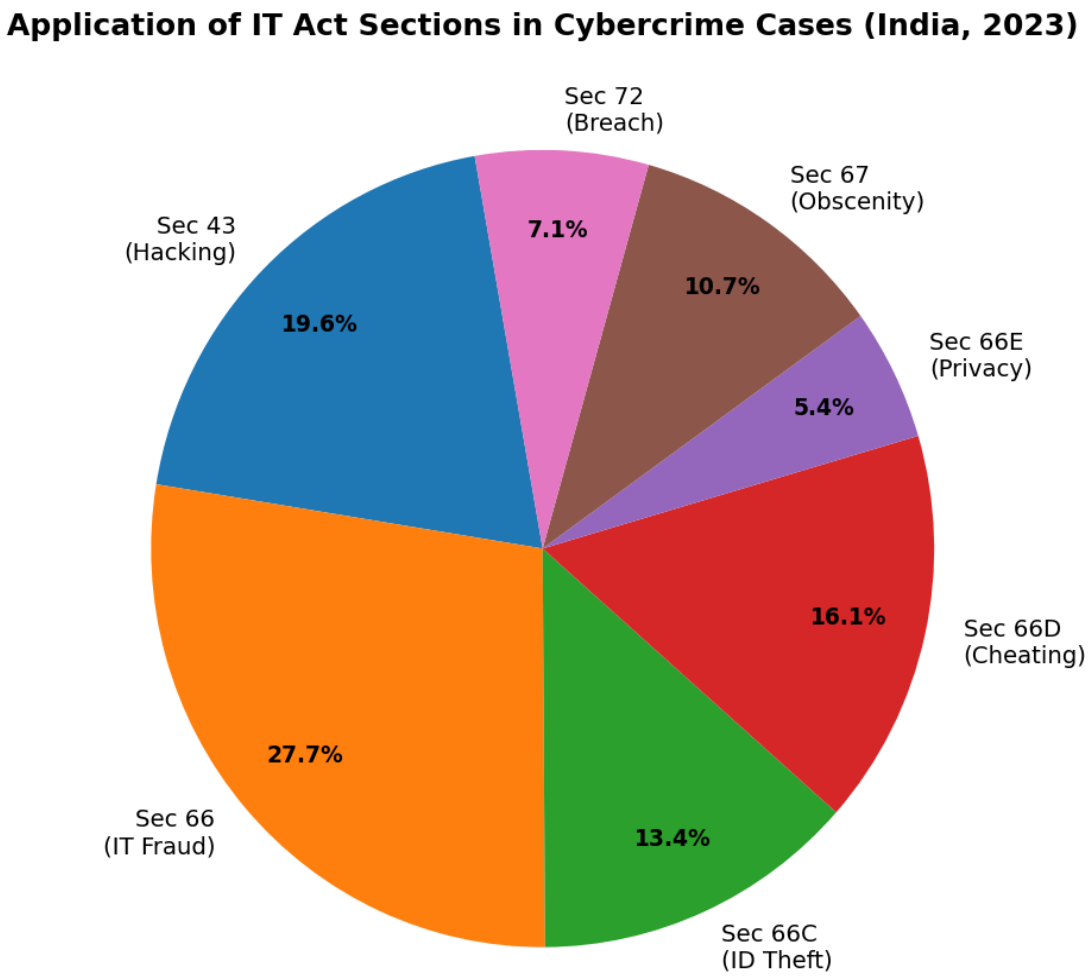

Figure 2: Application of IT Act Sections in Cybercrime Cases (India, 2023) — Source: NCRB Cybercrime Statistics 2023

2.2 Critical Gaps in the IT Act Framework

- Technological obsolescence: The Act predates social media, smartphones, cloud computing, cryptocurrency, ransomware, and AI-generated deepfakes.
- Definitional inadequacy: The Act's definitions do not encompass IoT devices, industrial control systems, or distributed ledger technologies.
- Jurisdictional lacunae: While Section 75 establishes extra-territorial jurisdiction, practical enforcement against foreign cybercriminals remains largely ineffective.
- Penalty disparities: Penalties under the IT Act are significantly lower than comparable offences under the IPC, creating anomalies in sentencing.

ISSN: 2582-6433

IT Act Section	Offence	Max Imprisonment	Max Fine	BNS Counterpart
Sec. 43	Unauthorised Access / Damage	Civil Remedy Only	No Cap	Sec. 316(2) BNS
Sec. 66	Computer-Related Offences	3 Years	Rs.5 Lakh	Sec. 316(3) BNS
Sec. 66C	Identity Theft	3 Years	Rs.1 Lakh	Sec. 319(1) BNS
Sec. 66D	Cheating by Personation	3 Years	Rs.1 Lakh	Sec. 319(2) BNS
Sec. 66E	Violation of Privacy	3 Years	Rs.2 Lakh	Sec. 317 BNS
Sec. 66F	Cyber Terrorism	Life Imprisonment	Unlimited	Sec. 302 BNS
Sec. 67	Obscene Content Publication	5 Years	Rs.10 Lakh	Sec. 294 BNS

Table 1: Key IT Act Cybercrime Offences and Corresponding BNS Provisions (2024)

3. DIGITAL EVIDENCE: THE SECTION 65B CONTROVERSY

The admissibility of electronic evidence in Indian courts is governed primarily by Sections 65A and 65B of the Indian Evidence Act 1872 (IEA), inserted by the Information Technology Act 2000. These provisions have generated some of the most significant and contentious judicial debate in Indian evidence law over the past two decades.

3.1 Section 65B: Statutory Framework

Section 65A provides that the contents of electronic records may be proved in accordance with Section 65B. Section 65B(1) stipulates that a printout, copy, or output of an electronic record is deemed to be a document and admissible as evidence without further proof, subject to four conditions: (i) the information was produced by activities of regular use during the ordinary course of activities; (ii) the computer was in regular use during the relevant period; (iii) the information was fed into the computer in the ordinary course of activities; and (iv) the computer was operating properly.

Section 65B(4) requires a certificate from a person occupying a responsible official position in relation to the operation of the relevant device or management of the relevant activities, certifying compliance with the above conditions. This certificate requirement has been the source of most judicial controversy.

 ISSN: 2582-6433

3.2 Landmark Judicial Interpretations

Anvar P.V. v P.K. Basheer (2014) 10 SCC 473: The Supreme Court held that Section 65B is a complete code for the admissibility of electronic evidence, overruling the earlier Afsan Guru decision. The Court mandated that a 65B certificate is an absolute prerequisite for the admissibility of electronic records. This decision created significant practical difficulties, as the certificate must be obtained from persons who may be unavailable, uncooperative, or lacking technical knowledge.

Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1: The Supreme Court revisited the 65B issue, holding that the certificate is mandatory only for the proponent of electronic evidence, that courts have the power to compel production of the 65B certificate, and that objections to admissibility must be taken at the time of tendering, not at the appellate stage.

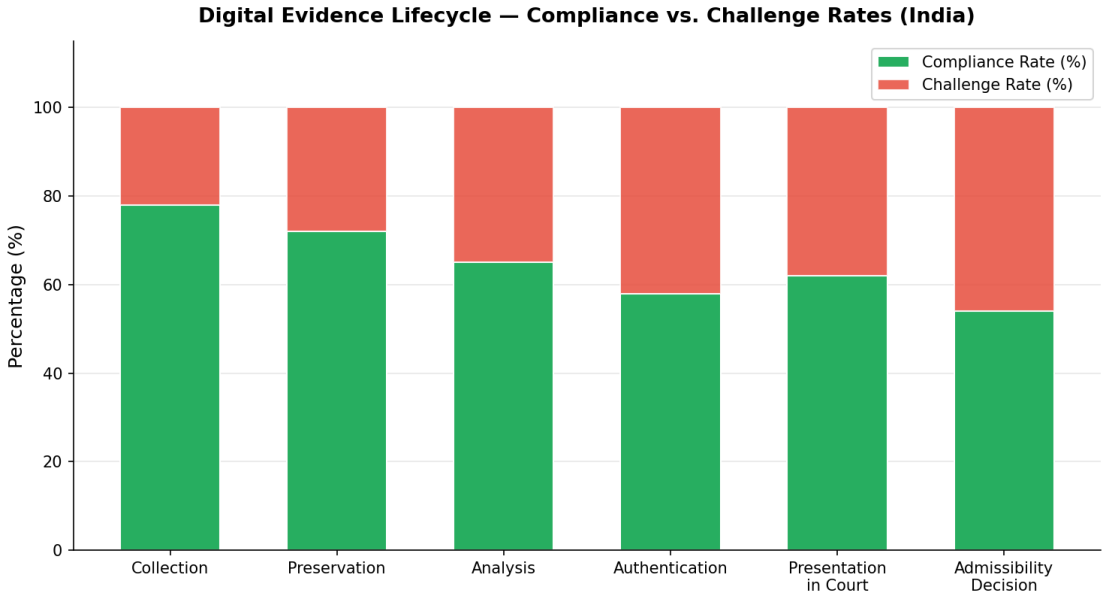

Figure 3: Digital Evidence Lifecycle — Compliance vs. Challenge Rates in Indian Courts — Source: Survey of High Court Records (2020–2024)

3.3 The Bharatiya Sakshya Adhiniyam 2023: Reforming Digital Evidence Law

The Bharatiya Sakshya Adhiniyam 2023 (BSA), which replaces the Indian Evidence Act from 1 July 2024, makes several important modifications to the digital evidence framework. Most significantly, Section 63 of the BSA modifies the certificate requirement to allow the certificate to be issued by 'any person who can provide such certificate.' This liberalisation addresses the practical difficulty of obtaining certificates from system operators and intermediaries. The BSA also introduces provisions for cloud-stored evidence and expands the definition of 'electronic

 ISSN: 2582-6433

record' to encompass IoT device data, CCTV recordings, and metadata.

4. TYPES OF CYBERCRIME AND LEGAL RESPONSE

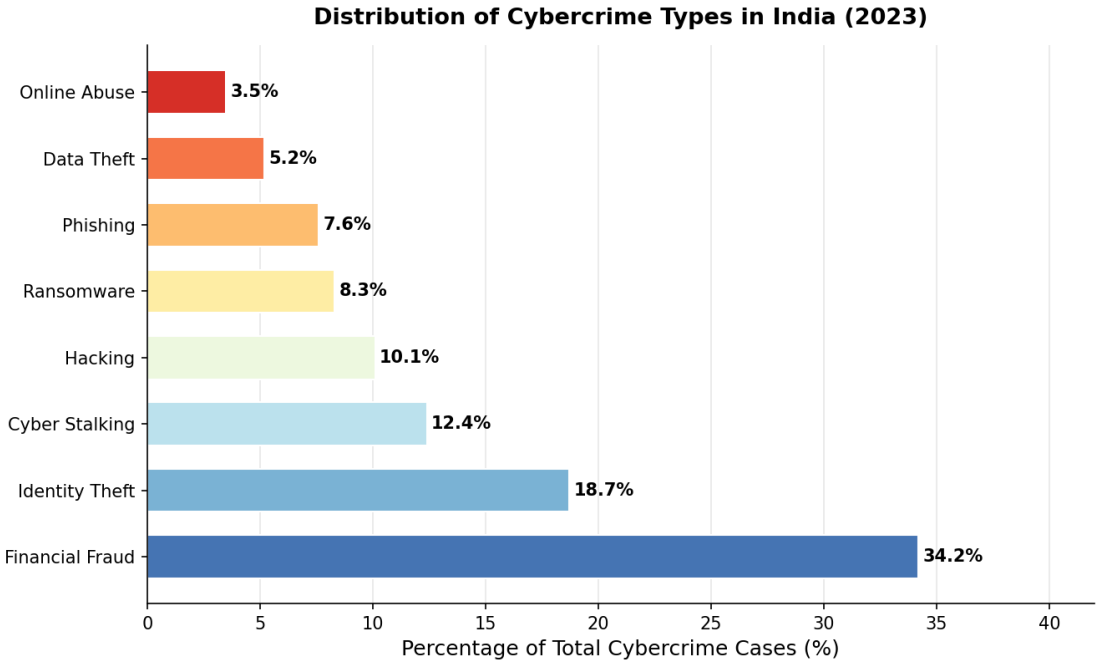

Figure 4: Distribution of Cybercrime Types in India (2023) — Source: NCRB Crime in India Report 2023

4.1 Financial Cybercrime

Financial cybercrime, encompassing online banking fraud, UPI fraud, investment scams, and credit card fraud, represents the largest category of cybercrime in India by volume and monetary impact. In 2023, the Indian Cybercrime Coordination Centre (I4C) under the Ministry of Home Affairs received over 15 lakh financial fraud complaints, involving losses exceeding Rs.26,000 crore. The primary legal mechanisms for addressing financial cybercrime include Sections 66C, 66D, and 420 IPC / Sections 316, 319 BNS, supplemented by the Payments and Settlement Systems Act 2007 and RBI circulars on electronic payment security.

4.2 Ransomware and Critical Infrastructure Attacks

India has been the target of significant ransomware attacks, including the 2022 AIIMS Delhi cyberattack and the 2023 CoWIN data breach. These incidents, while meeting the threshold for cyber terrorism under Section 66F of the IT Act (which provides for life imprisonment for attacks on national critical information infrastructure), have rarely resulted in successful prosecution due to attribution challenges inherent in state-sponsored or sophisticated criminal

ISSN: 2582-6433

group attacks.

4.3 Cyber Stalking, Online Harassment, and Deepfakes

Cyber stalking and online harassment, disproportionately targeting women and marginalised communities, represent a rapidly growing category of cybercrime with significant underreporting due to stigma, procedural complexity, and victim distrust in the justice system. The emergence of AI-generated deepfakes creates additional liability questions under Sections 66E, 67 IT Act and the potentially applicable tort of misappropriation of personality rights.

5. JURISDICTIONAL CHALLENGES AND INTERNATIONAL COOPERATION

5.1 Jurisdictional Framework Under the IT Act

Section 1(2) read with Section 75 of the IT Act establishes extra-territorial jurisdiction over cybercrimes committed outside India where the computer system involved is located in India. However, the practical exercise of extra-territorial jurisdiction is severely constrained by the sovereign immunity of foreign states, the absence of bilateral cybercrime extradition treaties with most major cybercrime source countries, and technical challenges in attributing attacks to specific foreign actors.

5.2 The Budapest Convention: India's Position

The Budapest Convention, to which over 65 states are parties as of 2024, provides a standardised framework for cybercrime substantive law and mutual legal assistance. India's non-participation has been justified on grounds of sovereignty concerns. However, India's absence from this treaty framework has materially impeded law enforcement cooperation in cross-border investigations, a concern underscored by the increasing origin of cyberattacks on India from Southeast Asian cybercrime hubs.

6. INVESTIGATIVE FRAMEWORK AND FORENSIC CHALLENGES

6.1 Police Powers Under the IT Act

The IT Act 2000 vests investigating powers in Police Officers of or above the rank of Inspector (Section 78), and designated officers of the Controller of Certifying Authorities and the Adjudicating Officer. Significant investigative powers include: search and seizure of computer systems (Sections 80, 69B); blocking of online content (Section 69A); interception of

ISSN: 2582-6433

electronic communications (Section 69); and the power to call for information from intermediaries.

6.2 Digital Forensics Infrastructure: Status and Gaps

India's digital forensics infrastructure, while growing, remains significantly underdeveloped relative to the scale of cybercrime. The Central Forensic Science Laboratory (CFSL) and state Forensic Science Laboratories suffer from severe capacity shortfalls. India has an estimated 1 digital forensics expert per 500,000 internet users, compared to 1 per 50,000 in developed countries. This deficit results in case backlogs, evidence degradation, and inadequate technical support for law enforcement investigations.

Challenge Area	Current Status	Impact on Prosecution	Recommended Reform
Digital Forensics Capacity	1 expert per 500K users	Case backlogs; evidence degradation	National Digital Forensics Training Academy
Chain of Custody	No standardised procedure	Admissibility challenges	Statutory evidence handling protocol
Cloud Evidence	No legal framework	Critical evidence inaccessible	Data Access Agreements with cloud providers
Encrypted Communications	Legal framework unclear	Law enforcement access blocked	Lawful access legislation with judicial oversight
MLAT Framework	Non-party to Budapest Convention	Slow MLA process (avg. 18 months)	Bilateral and multilateral treaty accession

Table 2: Key Challenges in Cybercrime Investigation and Prosecution in India

7. POLICY RECOMMENDATIONS AND THE WAY FORWARD

7.1 Legislative Reforms

- Enactment of a dedicated Cybercrime Investigation and Digital Evidence Act to consolidate the fragmented legal framework, incorporating updated definitions, expanded offences (ransomware, crypto-crimes, AI deepfakes), and standardised digital forensics procedures.

ISSN: 2582-6433

- India should accede to or seek a parallel instrument to the Budapest Convention to facilitate mutual legal assistance in cybercrime investigations.
- A specific legal framework addressing AI-generated deepfakes, including criminal liability for malicious creation and distribution, civil remedies for victims, and platform liability for hosting deepfake content without consent.

7.2 Institutional and Capacity Building

- Establishment of a National Digital Forensics Academy to train and certify digital forensics examiners to international standards.
- Creation of specialised Cybercrime Courts in all District Courts with trained judges and technology experts as court assessors.
- A National Victim Assistance Fund for cybercrime victims, funded by penalties collected under the IT Act and DPDPA.
- Mandatory digital literacy programmes in all schools and tertiary institutions.

8. CONCLUSION

Cybercrime represents one of the most pressing and complex challenges facing India's legal system in the digital age. The dramatic escalation in both the volume and sophistication of cybercrime has outpaced the development of India's legal and institutional response. The result is a significant 'justice gap' that leaves victims without adequate redress, emboldens perpetrators through low conviction rates, and threatens the security of India's critical digital infrastructure.

India requires a comprehensive, multi-dimensional response: legislative modernisation through a dedicated Cybercrime Act; institutional strengthening through specialised courts and forensic academies; international engagement through treaty accession and bilateral cooperation agreements; and public education through digital literacy initiatives. The constitutionalisation of privacy under Puttaswamy creates both an obligation and an opportunity to build a cybercrime legal framework that simultaneously protects citizen privacy, ensures law enforcement efficacy, and upholds the rule of law in cyberspace.

ISSN: 2582-6433

REFERENCES

1. *Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (Supreme Court of India).*
2. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (Supreme Court of India).*
3. *Sonu @ Amar v. State of Haryana, (2017) 8 SCC 570 (Supreme Court of India).*
4. *National Crime Records Bureau. (2023). Crime in India 2022. Ministry of Home Affairs, Government of India.*
5. *CERT-In. (2024). Annual Report 2023: Cyber Security Incidents in India. Indian Computer Emergency Response Team.*
6. *Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). ETS No. 185.*
7. *Information Technology Act, 2000. (Act 21 of 2000, as amended 2008). Government of India.*
8. *Bharatiya Nyaya Sanhita, 2023. (Act 45 of 2023). Government of India.*
9. *Bharatiya Sakshya Adhiniyam, 2023. (Act 47 of 2023). Government of India.*
10. *Ministry of Home Affairs. (2024). Annual Report on Cyber Crime 2023. Indian Cybercrime Coordination Centre (I4C).*
11. *Sinha, A. (2023). Digital Evidence and the Indian Criminal Justice System. Indian Law Review, 7(3), 211-248.*
12. *Rajaraman, V. (2022). Cybercrime Investigation in India: Challenges and Solutions. Journal of Cyber Law, 8(1), 44-78.*
13. *IBM Security. (2024). Cost of a Data Breach Report — India Edition 2024. IBM Corporation.*
14. *UNODC. (2023). Cybercrime and the Use of Digital Evidence in South Asia. United Nations Office on Drugs and Crime.*
15. *Pavan Duggal. (2023). Commentary on the Information Technology Act. Lexis Nexis India, New Delhi.*