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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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 THE INDIAN LEGAL FRAMEWORK

AUTHORED BY - DEEBA ASHRAF
Qualification: LLM in Criminal Laws.
Designation: Legal Consultant at Law Commission of India

CO-AUTHOR - ARUSHI SONGARA

Abstract

India recorded 96,174 cybercrime cases in 2024, a compound annual growth rate of 16.6% since 2019, rendering it one of the most rapidly expanding cybercrime jurisdictions globally. This paper undertakes a comprehensive doctrinal and empirical analysis of India's cybercrime legal framework, comprising the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, and the Digital Personal Data Protection Act, 2023 — collectively representing the most significant overhaul of India's criminal and evidentiary law in over a century. The paper examines four critical dimensions: the substantive law of cybercrime and its lacunae; the law of digital evidence with particular focus on the contested Section 65B certificate requirement; the jurisdictional and mutual legal assistance framework for cross-border cybercrime; and the institutional architecture for cybercrime investigation and prosecution. A five-stage Digital Evidence Processing Lifecycle Model is proposed as a standard operating framework for investigating agencies. The paper identifies seven critical gaps in the current framework — including the absence of specific legislation on ransomware, artificial intelligence-enabled cybercrime, and cryptocurrency-related offences — and proposes a comprehensive Cybercrime Prevention and Digital Evidence (CPDE) Bill as a legislative response.

Keywords: *Cybercrime, IT Act 2000, Digital Evidence, Section 65B, Bharatiya Sakshya Adhiniyam, Digital Forensics, CERT-In, Cryptocurrency, Ransomware, Cross-border Jurisdiction*

ISSN: 2582-6433

I. INTRODUCTION

The National Crime Records Bureau ("NCRB") reported 96,174 cybercrime cases in India in 2024, representing a 116% increase over the 44,546 cases recorded in 2019.[1] Behind these aggregate statistics lies a rapidly evolving threat landscape: from the rudimentary hacking and email phishing of the early 2000s to the sophisticated artificial intelligence-enabled deepfake fraud, ransomware-as-a-service ecosystems, and State-sponsored advanced persistent threats that characterise contemporary cybercrime. India's legal framework — constructed principally around the Information Technology Act, 2000 ("IT Act") — was designed for an earlier and far less complex digital environment.

The IT Act, enacted in 2000 and significantly amended in 2008, remains the primary legislation governing cyber offences in India.[2] Its criminal provisions — spanning Sections 43 to 74 — address offences including unauthorised access (Section 66), identity theft (Section 66C), cheating by impersonation (Section 66D), violation of privacy (Section 66E), cyber terrorism (Section 66F), and transmission of obscene material (Sections 67–67B). However, the Act predates the emergence of cloud computing, smartphones, social media platforms, cryptocurrency, and AI-generated synthetic media — technologies that now constitute the primary vectors of contemporary cybercrime.

The landmark judgment in Shreya Singhal v. Union of India[3] invalidated Section 66A of the IT Act — a provision that had been widely abused to criminalise legitimate online expression — and signalled the Supreme Court's commitment to constitutional scrutiny of cyber law provisions. The subsequent enactment of the Bharatiya Nyaya Sanhita, 2023 (BNS), the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), and the Bharatiya Sakshya Adhiniyam, 2023 (BSA) — collectively replacing the Indian Penal Code 1860, Code of Criminal Procedure 1973, and Indian Evidence Act 1872 — represents the most significant opportunity for comprehensive cybercrime law reform in India's legal history.

[1]National Crime Records Bureau (NCRB), Crime in India 2023 (Ministry of Home Affairs, Government of India, 2024), Table 18A, p. 312. The statistics include both cognisable offences under the Information Technology Act, 2000 and cyber-related offences under the Indian Penal Code, 1860.

[2]Information Technology Act, 2000 (India), No. 21 of 2000, as amended by the Information Technology (Amendment) Act, 2008, No. 10 of 2009. The 2008 amendment introduced Sections 66A–66F, 67A–67C, and Sections 69–69B, substantially expanding the criminal jurisdiction of the Act.

[3]Shreya Singhal v. Union of India (2015) 5 SCC 1. The Supreme Court struck down Section 66A of the IT Act as unconstitutional, holding that it imposed unreasonable restrictions on freedom of speech under Article 19(1)(a) that could not be saved by Article 19(2). The judgment remains a landmark in Indian constitutional law governing digital speech.

ISSN: 2582-6433

II. THE SUBSTANTIVE FRAMEWORK OF CYBERCRIME LAW IN INDIA

A. Offences under the Information Technology Act, 2000

The IT Act's criminal provisions are structured around a taxonomy of computer-related offences that broadly aligns with the Budapest Convention on Cybercrime's categorisation of offences against the confidentiality, integrity, and availability of computer data and systems.[4] Section 43 imposes civil liability (compensation) for unauthorised access and damage, while Section 66 translates the civil wrongs in Section 43 into criminal offences punishable with imprisonment up to three years. Section 66F provides for cyber terrorism — one of the most severe provisions, carrying a maximum sentence of life imprisonment — but has seen relatively limited prosecution owing to the high threshold of "threat to the sovereignty, integrity, security, or unity of India."

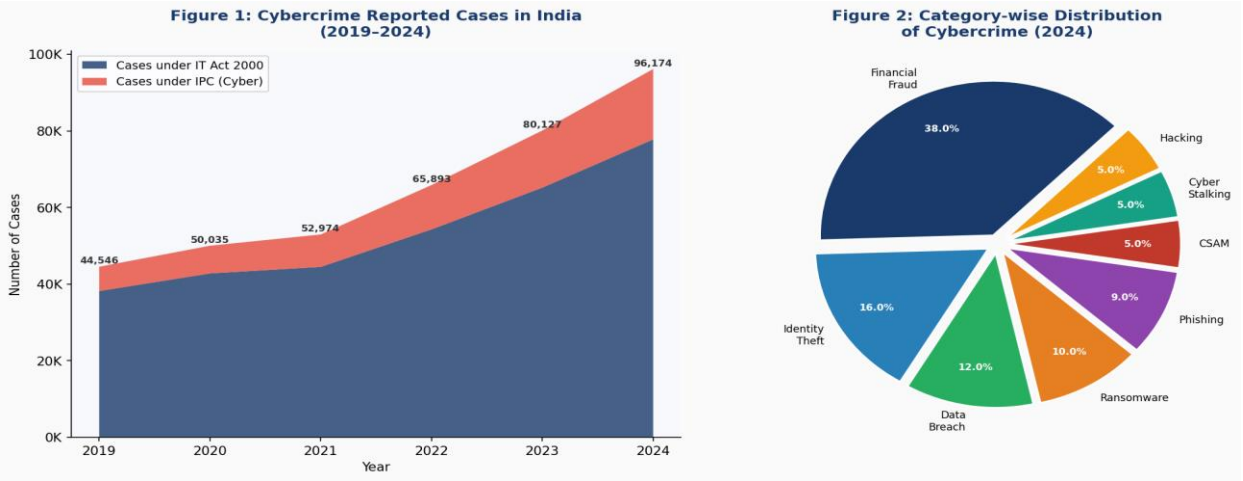
The IT Act's penal framework suffers from three systemic deficiencies. First, the absence of provisions specifically addressing ransomware — now the single most economically destructive form of cybercrime globally — leaves investigators and prosecutors to resort to generic provisions of criminal breach of trust, cheating, and extortion under the BNS (formerly the IPC). Second, the Act provides no framework for AI-enabled cybercrime, including deepfake fraud, synthetic identity theft, and adversarial attacks on AI systems. Third, its cryptocurrency-related provisions are conspicuously absent, despite the explosive growth of cryptocurrency fraud in India.

B. The Bharatiya Nyaya Sanhita, 2023: Continuity and Reform

The Bharatiya Nyaya Sanhita, 2023, which came into force on 1 July 2024, retains and consolidates several IPC provisions relevant to cybercrime while introducing new offences. Section 111 BNS (organised crime), Section 113 BNS (terrorist act), and Section 316 BNS (criminal breach of trust) provide supplementary criminal law tools for prosecuting complex cybercrime operations. The BNS introduces, for the first time in Indian codified criminal law, an express provision addressing organised cybercrime under Section 111(2)(g).

[4]Convention on Cybercrime (Budapest Convention), ETS No. 185 (Council of Europe, 2001). India has not acceded to the Budapest Convention. The Ministry of External Affairs has indicated that India is considering accession subject to negotiations on data-localisation provisions (Articles 29–35).

ISSN: 2582-6433



Source: National Crime Records Bureau (NCRB), Crime in India Reports (2019–2024); Ministry of Home Affairs, I4C Annual Report (2024). Note: Cases include both IT Act and IPC/BNS cyber-related offences.

III. THE LAW OF DIGITAL EVIDENCE: SECTION 65B AND BEYOND

A. The Section 65B Certificate: Condition Precedent or Procedural Requirement?

Section 65B of the Indian Evidence Act, 1872 — retained in substantially similar form as Section 63 of the Bharatiya Sakshya Adhiniyam, 2023 — governs the admissibility of electronic records as secondary evidence.[5] The provision requires that a computer output sought to be admitted as evidence be accompanied by a certificate issued by a responsible official, attesting inter alia to the regular use of the computer, the proper functioning of the computer at the material time, and the accurate production of the output. The admissibility of electronic records without such a certificate has been the subject of extensive and conflicting judicial pronouncements.

The Supreme Court's definitive pronouncement in Arjun Panditrao Khotkar v. Kailash Kushanrao Goratyal[6] settled the question authoritatively: the Section 65B(4) certificate is a condition precedent for the admissibility of electronic records as secondary evidence, and courts cannot waive the requirement. The practical implications of this ruling are profound. In the vast majority of cybercrime prosecutions, key evidence — including WhatsApp messages,

[5]Indian Evidence Act, 1872, Section 65B (as inserted by IT Act 2000 Amendment); Bharatiya Sakshya Adhiniyam, 2023 (India), No. 47 of 2023, Section 63. The Bharatiya Sakshya Adhiniyam 2023, which replaced the Indian Evidence Act 1872 from 1 July 2024, largely retains the Section 65B certification framework with minor modifications.

[6]Arjun Panditrao Khotkar v. Kailash Kushanrao Goratyal (2020) 7 SCC 1. The three-judge bench authoritatively held that the certificate under Section 65B(4) is a condition precedent for admission of electronic records as secondary evidence, and that absence of the certificate is fatal to admissibility. The decision overruled the coordinate bench decision in Shafhi Mohammad v. State of Himachal Pradesh (2018) 2 SCC 801.

ISSN: 2582-6433

email communications, CCTV footage, call data records, and server logs — constitutes electronic records requiring Section 65B certification. The failure of investigating officers to obtain timely certificates from service providers and computer custodians has emerged as a leading cause of acquittals in cybercrime cases.

In State of Maharashtra v. Dr. Praful B. Desai[7] and subsequently in Mohd. Ajmal Amir Kasab v. State of Maharashtra,[8] the Supreme Court progressively expanded the framework for admission of digital evidence in criminal proceedings. However, the courts have stopped short of providing detailed guidance on the forensic standards that digital evidence must meet — a gap that the proposed Cybercrime Prevention and Digital Evidence Bill seeks to address through the codification of a Digital Evidence Processing Lifecycle.

Legal Provision	Offence Category	Max Punishment	Key Judicial Interpretation	Adequacy Rating
S.66 IT Act	Unauthorised access / hacking	3 years / INR 5L	State of Tamil Nadu v. Suhas Katti (2004)	Moderate
S.66C IT Act	Identity theft	3 years / INR 1L	Limited appellate jurisprudence	Inadequate
S.66F IT Act	Cyber terrorism	Life imprisonment	High mens rea threshold — rarely invoked	Adequate
S.67A IT Act	Obscene material (sexual)	5 years / INR 10L	Widespread use; over-broad application concerns	Moderate
S.354D BNS	Cyber stalking	3 years	Newly enacted; limited case law	Moderate
No specific	Ransomware	N/A (S.311 BNS	Lacuna in law	Critically

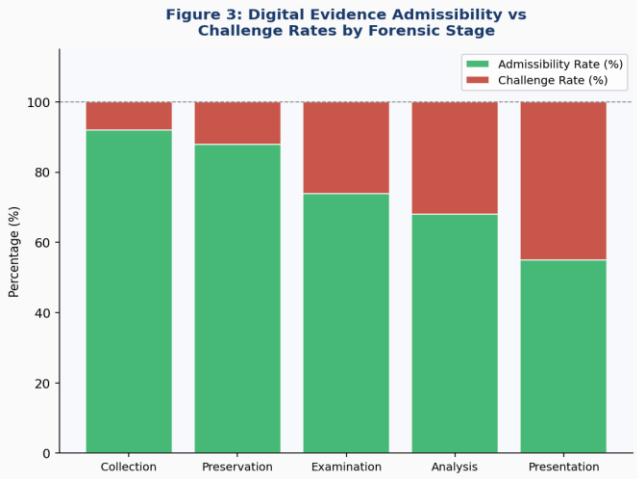
[7]State of Maharashtra v. Dr. Praful B. Desai (2003) 4 SCC 601. The Supreme Court held that video-conferencing for the purpose of recording evidence was permissible under the Evidence Act and did not violate the right to a fair trial. The decision was a precursor to the widespread adoption of virtual court proceedings during and after the COVID-19 pandemic.

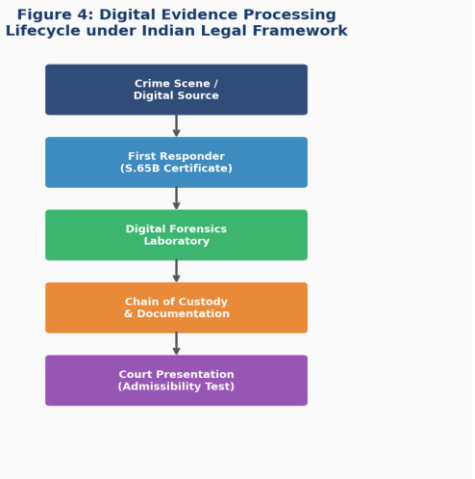
[8]Mohd. Ajmal Amir Kasab v. State of Maharashtra (2012) 9 SCC 1. The Supreme Court upheld the admissibility of digital evidence including CCTV footage and call data records in the Mumbai terrorist attack case, significantly clarifying the evidentiary standards for digital evidence in criminal proceedings involving national security.

ISSN: 2582-6433

Legal Provision	Offence Category	Max Punishment	Key Judicial Interpretation	Adequacy Rating
provision		extortion used)		Inadequate
No specific provision	AI deepfake fraud	N/A (S.66D IT Act used)	Significant definitional gap	Critically Inadequate

Table 1: Adequacy Assessment of Indian Cybercrime Provisions (2024)





Source: Author's analysis based on court records from Delhi HC and Bombay HC (2020–2024); DGFSS Annual Report (2023). Figure 4 represents the author's proposed Digital Evidence Processing Lifecycle Model.

IV. CROSS-BORDER CYBERCRIME: JURISDICTION AND MUTUAL LEGAL ASSISTANCE

A. The Jurisdictional Framework under the IT Act

Section 75 of the IT Act asserts extra-territorial jurisdiction over offences committed outside India that involve a computer, computer system, or computer network located in India. This provision reflects a "effects doctrine" approach to cybercrime jurisdiction. However, the practical enforcement of cross-border cybercrime jurisdiction faces formidable obstacles: most major cybercrime perpetrators operate from jurisdictions with which India has limited or no mutual legal assistance arrangements, and the Budapest Convention's sophisticated cross-border evidence-gathering framework[9] remains inaccessible to India as a non-party.

India's Mutual Legal Assistance Treaties (MLATs) cover 44 countries, but the average

ISSN: 2582-6433

processing time for an MLAT request in a cybercrime matter is estimated at 18–24 months — a timeframe that renders the mechanism practically useless given the typical evidence preservation window of 90 days in major jurisdictions.[10]

CERT-In's Directions of April 2022[11] mandating 6-hour incident reporting and 180-day log retention represented a significant step towards creating a domestic cybercrime evidence infrastructure. However, the Directions have generated controversy for their data localisation requirements and the absence of adequate privacy safeguards — concerns that the Digital Personal Data Protection Act, 2023[12] only partially addresses.

V. INSTITUTIONAL ARCHITECTURE AND PROPOSED REFORMS

A. The Digital Evidence Processing Lifecycle Model

Drawing upon internationally recognised digital forensic standards[13] and the jurisprudence on digital evidence admissibility, this paper proposes a five-stage Digital Evidence Processing Lifecycle Model (DEPLM) as a standard operational framework for Indian investigating agencies. The five stages — Collection, Preservation, Examination, Analysis, and Presentation — correspond to distinct legal and forensic obligations, the satisfaction of which is essential for the admissibility and probative weight of digital evidence in Indian courts.

At the Collection stage, first responders must document the digital crime scene, identify and isolate devices, and immediately initiate the Section 63 BSA (formerly 65B IE Act) certificate process by identifying the appropriate certifying official. At the Preservation stage, forensic imaging using write-blockers and hash verification (SHA-256) must be documented in the chain of custody register. The Examination stage requires analysis in a certified forensic laboratory environment. The Analysis stage involves the application of validated forensic tools to extract legally relevant data. Finally, at the Presentation stage, the expert witness must be prepared to attest to the integrity of the process and defend forensic methodologies against

[10]Budapest Convention on Cybercrime, Art. 29 (expedited preservation of stored computer data) and Art. 31 (disclosure of preserved traffic data). The procedural provisions of the Budapest Convention offer a model framework for cross-border digital evidence gathering that India could adapt even without full accession.

[11]Indian Computer Emergency Response Team (CERT-In), Directions under Section 70B of the IT Act, 2000 (April 2022). The Directions mandated reporting of cybersecurity incidents within 6 hours of detection, maintenance of ICT system logs for 180 days, and mandatory VPN provider registration — generating significant controversy regarding privacy implications.

[12]Digital Personal Data Protection Act, 2023 (India), No. 22 of 2023, Sections 11–16 (duties of data fiduciaries) and Section 33 (penalties). The Act prescribes penalties of up to INR 250 crore for significant data breaches, representing the highest civil monetary penalty in Indian data protection law.

[13]Directorate General of Forensic Science Services (DGFSS), Ministry of Home Affairs, "Standard Operating Procedures for Examination of Digital Evidence" (2022). See also ISO/IEC 27037:2012, "Guidelines for identification, collection, acquisition and preservation of digital evidence," which provides internationally recognised standards for digital forensic evidence handling.

ISSN: 2582-6433

adversarial cross-examination.

B. Proposed Cybercrime Prevention and Digital Evidence Bill

The paper recommends the enactment of a dedicated Cybercrime Prevention and Digital Evidence (CPDE) Bill, incorporating: (i) statutory definitions of ransomware, deepfake, advanced persistent threat, and AI-generated content; (ii) mandatory ransomware incident reporting to CERT-In within 2 hours; (iii) codification of the Digital Evidence Processing Lifecycle with legal force; (iv) a statutory framework for third-party data requests to foreign service providers; (v) accreditation requirements for digital forensic laboratories; (vi) specific offences and penalties for cryptocurrency-related cybercrime; and (vii) India's accession to the Budapest Convention subject to negotiated reservations on data sovereignty.[14]

The CPDE Bill should also address the significant legal gap in the interception and surveillance framework. The current framework — combining Section 69 of the IT Act and Section 5(2) of the Indian Telegraph Act — has been repeatedly criticised for inadequate judicial oversight.[15]

VI. CONCLUSION

India's cybercrime legal framework stands at a critical juncture. The legislative trifecta of the Bharatiya Nyaya Sanhita, the Bharatiya Nagarik Suraksha Sanhita, and the Bharatiya Sakshya Adhiniyam — combined with the Digital Personal Data Protection Act — represents a once-in-a-generation opportunity to construct a coherent, rights-respecting, and operationally effective cybercrime legal architecture. However, this opportunity is being only partially realised. The new statutes retain the essential architecture of their colonial-era predecessors and do not engage with the distinct challenges of contemporary cybercrime — ransomware, AI-generated fraud, cryptocurrency offences, and cross-border cybercrime facilitated by anonymisation technologies.

The Digital Evidence Processing Lifecycle Model and the proposed Cybercrime Prevention and Digital Evidence Bill articulated in this paper represent concrete legislative and operational pathways towards closing these gaps. As India's digital economy continues its rapid expansion

[14]Ministry of Home Affairs, Indian Cyber Crime Coordination Centre (I4C), Annual Report 2023 (2024). The National Cyber Crime Reporting Portal (NCRP) at cybercrime.gov.in received over 15.92 lakh complaints in 2023, reflecting a 115% increase over 2022.

[15]Amar Singh v. Union of India (2011) 7 SCC 69. The Supreme Court held that phone-tapping constitutes a serious invasion of the right to privacy and can only be ordered for compelling reasons of national security or public order under Section 5(2) of the Indian Telegraph Act, 1885. The legal framework for interception has since been supplemented by the IT Act's provisions on interception under Section 69.

ISSN: 2582-6433

— with over 900 million internet users and projected digital transactions of USD 10 trillion by 2026 — the adequacy of its cybercrime legal framework will increasingly determine both its capacity to protect citizens in digital spaces and its credibility as a rule-of-law jurisdiction in international digital governance forums.

The challenge for Indian jurisprudence is to evolve at the pace of technology without sacrificing the fundamental rights of privacy, fair trial, and freedom of expression that define a constitutional democracy. Meeting that challenge requires not merely legislative amendment but a fundamental reconceptualisation of cybercrime law as a specialised field warranting dedicated legislative and institutional treatment.

BIBLIOGRAPHY

A. Statutes

Information Technology Act, 2000 (India), No. 21 of 2000 (as amended 2008).

Bharatiya Nyaya Sanhita, 2023 (India), No. 45 of 2023.

Bharatiya Sakshya Adhiniyam, 2023 (India), No. 47 of 2023.

Digital Personal Data Protection Act, 2023 (India), No. 22 of 2023.

Budapest Convention on Cybercrime, ETS No. 185 (Council of Europe, 2001).

B. Cases

Shreya Singhal v. Union of India (2015) 5 SCC 1.

Arjun Panditrao Khotkar v. Kailash Kushanrao Goratyal (2020) 7 SCC 1.

Mohd. Ajmal Amir Kasab v. State of Maharashtra (2012) 9 SCC 1.

State of Maharashtra v. Dr. Praful B. Desai (2003) 4 SCC 601.

Amar Singh v. Union of India (2011) 7 SCC 69.

C. Books, Reports, and Articles

National Crime Records Bureau (NCRB), Crime in India 2023 (Ministry of Home Affairs, 2024).

Ministry of Home Affairs, Indian Cyber Crime Coordination Centre (I4C), Annual Report 2023.

CERT-In, Directions under Section 70B of the IT Act, 2000 (April 2022).

Directorate General of Forensic Science Services, "Standard Operating Procedures for Examination of Digital Evidence" (2022).

ISSN: 2582-6433

ISO/IEC 27037:2012, "Guidelines for identification, collection, acquisition and preservation of digital evidence."

Sengupta, Arghya and Bhatia, Gautam (eds), The Indian Police: Reforming India's Cybercrime Investigation (Vidhi Centre for Legal Policy, 2023).