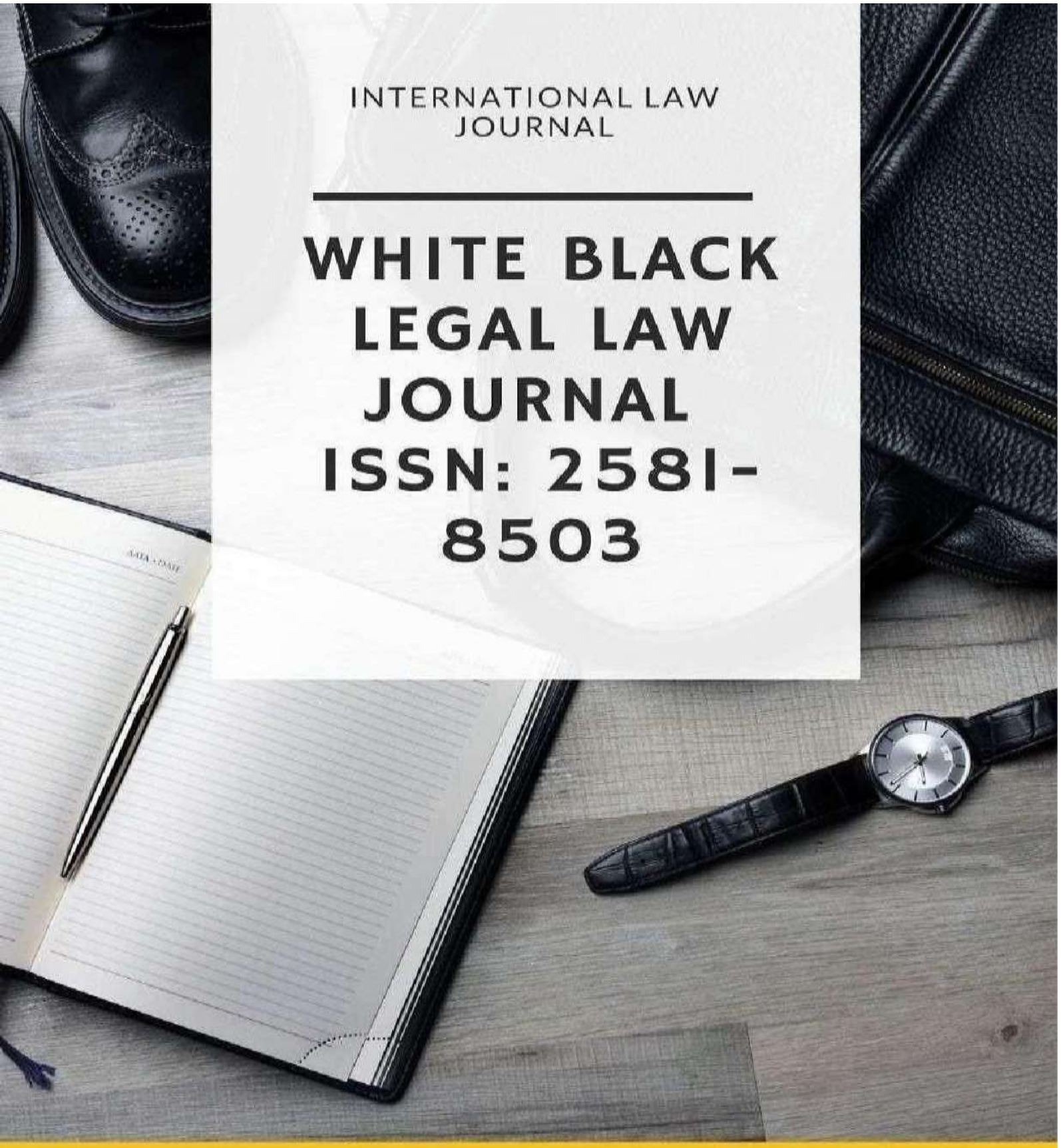

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, translated, or distributed in any form or by any means—whether electronic, mechanical, photocopying, recording, scanning, or otherwise—without the prior written permission of the Editor-in-Chief of *White Black Legal – The Law Journal*.

All copyrights in the articles published in this journal vest with *White Black Legal – The Law Journal*, unless otherwise expressly stated. Authors are solely responsible for the originality, authenticity, accuracy, and legality of the content submitted and published.

The views, opinions, interpretations, and conclusions expressed in the articles are exclusively those of the respective authors. They do not represent or reflect the views of the Editorial Board, Editors, Reviewers, Advisors, Publisher, or Management of *White Black Legal*.

While reasonable efforts are made to ensure academic quality and accuracy through editorial and peer-review processes, *White Black Legal* makes no representations or warranties, express or implied, regarding the completeness, accuracy, reliability, or suitability of the content published. The journal shall not be liable for any errors, omissions, inaccuracies, or consequences arising from the use, interpretation, or reliance upon the information contained in this publication.

The content published in this journal is intended solely for academic and informational purposes and shall not be construed as legal advice, professional advice, or legal opinion. *White Black Legal* expressly disclaims all liability for any loss, damage, claim, or legal consequence arising directly or indirectly from the use of any material published herein.

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

www.whiteblacklegal.co.in
Volume 3 Issue 4 | Feb 2026 ISSN: 2581-8503

EVIDENTIARY AND JURISDICTIONAL CHALLENGES IN CYBERCRIME PROSECUTION IN INDIA: A CRITICAL STUDY OF THE INFORMATION TECHNOLOGY ACT, 2000

AUTHORED BY - AMRESH MANI TRIPATHI & DR.KAVYA CHANDEL

Abstract

The rapid expansion of digital infrastructure in India has intensified the scale and sophistication of cybercrime, placing increasing strain on the criminal justice system. Cybercrime prosecution presently confronts two interrelated doctrinal challenges: evidentiary admissibility under Section 65B of the Indian Evidence Act, 1872, and jurisdictional enforcement under Section 75 of the Information Technology Act, 2000. Judicial inconsistency in the interpretation of certification requirements in *Anvar P.V. v. P.K. Basheer, Shafhi Mohammad v. State of Himachal Pradesh, and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal* has generated doctrinal uncertainty regarding the admissibility of electronic evidence.

Simultaneously, the borderless character of cyberspace complicates territorial competence and cross-border enforcement, exacerbated by procedural fragmentation and Mutual Legal Assistance inefficiencies. Through doctrinal and comparative analysis, this study identifies normative ambiguities and procedural gaps that weaken prosecutorial effectiveness and proposes calibrated reforms consistent with constitutional safeguards and evolving digital realities.

Keywords: Cybercrime; Electronic Evidence; Section 65B; Information Technology Act; Jurisdiction; Digital Forensics; Cross-border Enforcement; Budapest Convention

1. Introduction

The transformation of criminal activity through digital technologies has imposed unprecedented demands upon legal systems designed for a territorial, physical world. India, with over 900 million internet users and one of the world's largest digital economies, has

witnessed a corresponding escalation in cybercrime that challenges the foundational assumptions of criminal procedure.[1] The Information Technology Act, 2000, enacted to provide legal recognition for electronic transactions and address computer-related offences, has proven doctrinally inadequate to the evidentiary and jurisdictional complexities that characterize contemporary digital crime.

Two interconnected problems define the crisis in cybercrime prosecution. The first concerns the admissibility and authentication of electronic evidence under section 65B of the Indian Evidence Act, 1872, a provision whose interpretation has oscillated dramatically across Supreme Court decisions, producing a jurisprudence marked by internal contradiction rather than doctrinal stability. The second concerns the jurisdictional architecture of the Information Technology Act itself, particularly section 75, which asserts expansive extraterritorial application while remaining tethered to enforcement mechanisms incapable of transcending national boundaries. These are not merely technical difficulties susceptible to incremental adjustment; they represent structural deficiencies that compromise the legitimacy of criminal adjudication in the digital sphere.

The doctrinal stakes extend beyond procedural efficiency. Electronic evidence now constitutes the evidentiary foundation for prosecutions ranging from financial fraud to terrorism, from intellectual property theft to offences against women and children. When courts exclude such evidence on procedural technicalities divorced from reliability concerns, or when prosecutors cannot obtain evidence located on servers beyond Indian territorial jurisdiction, the criminal justice system fails in its fundamental obligation to adjudicate guilt and innocence on the merits. Conversely, when evidentiary standards are relaxed without adequate safeguards, or when jurisdictional assertions exceed legitimate sovereign authority, the rights of the accused suffer corresponding diminution. The challenge is not simply to facilitate prosecution but to construct a framework that reconciles investigative necessity with constitutional constraint.

This article addresses three research questions. First, does the current evidentiary frame- work for electronic records, as interpreted by the Supreme Court, provide technologically coherent and doctrinally consistent standards for admissibility? Second, does section 75 of the

[1] National Crime Records Bureau, *Crime in India 2022* (Ministry of Home Affairs, 2023). The NCRB recorded 65,893 cybercrime cases in 2022, representing a 24.4 per cent increase from the previous year, though these figures likely underrepresent actual incidence given significant underreporting.

Information Technology Act establish a jurisdictional architecture capable of effective enforcement against transnational cybercrime, or does it represent an aspirational assertion disconnected from procedural reality? Third, what legislative and institutional reforms would reconcile the competing demands of prosecutorial efficacy, technological accuracy, and constitutional rights protection?

The thesis advanced is that Indian law governing cybercrime prosecution suffers from a fundamental disjunction between statutory ambition and operational coherence. The evidentiary regime privileges formal certification over substantive reliability, while the jurisdictional framework asserts authority it cannot exercise. Reform requires not merely technical amendment but reconceptualization of how criminal law engages with digital phenomena a reconceptualization grounded in technological realism, comparative learning, and constitutional fidelity.

The methodology employed is doctrinal legal research, supplemented by case-law analysis and comparative evaluation. The analysis proceeds as follows: Part 2 examines the legislative architecture and normative foundations of cybercrime regulation. Part 3 undertakes critical examination of evidentiary challenges. Part 4 analyzes jurisdictional complexity. Part 5 provides comparative perspective. Part 6 offers institutional and doctrinal critique. Part 7 proposes concrete reforms. Part 8 concludes.

2. Legislative Architecture and Normative Foundations

2.1 Evolution of the Information Technology Act, 2000

The Information Technology Act, 2000 emerged from India's recognition that participation in the global digital economy required legal infrastructure for electronic commerce and governance. The Act drew upon the UNCITRAL Model Law on Electronic Commerce (1996), seeking to provide legal recognition for electronic records and digital signatures while establishing a framework for addressing computer-related offences.[2] The original enactment reflected the technological assumptions of its era a period when internet penetration in India remained minimal and the full implications of networked computing for criminal activity had not yet materialized.

[2] Statement of Objects and Reasons, Information Technology Bill, 1999. The legislative intent focused primarily on facilitating e-commerce rather than comprehensive cybercrime regulation.

The 2008 amendments represented a substantial expansion of the Act's criminal provi- sions, responding to the Mumbai terrorist attacks and growing awareness of cyber-enabled threats to national security.[3] These amendments introduced new offences including identity theft (section 66C), cheating by personation using computer resources (section 66D), violation of privacy (section 66E), and cyber terrorism (section 66F). The amendments also modified intermediary liability provisions and established the Indian Computer Emergency Response Team (CERT-In). Yet the 2008 amendments, while expanding substantive offences, did not adequately address the procedural and evidentiary difficulties that would increasingly constrain effective prosecution.

The legislative design reflects a fundamental tension between the Act's dual character as both a facilitative statute for electronic commerce and a penal statute for computer crime. This duality produces interpretive difficulties, as provisions drafted with commercial transactions in mind must be applied to criminal investigations requiring different procedural safeguards. The Act's definitions of "computer," "computer system," "computer network," and "data" in section 2, while technologically neutral in aspiration, have required continuous judicial adaptation to encompass smartphones, cloud computing, and distributed systems not contemplated by the original drafters.

2.2 Interplay with the Criminal Justice Framework

Cybercrime prosecution in India operates through an intricate relationship between the Information Technology Act and the general criminal law framework comprising the Indian Penal Code, 1860, the Code of Criminal Procedure, 1973, and the Indian Evidence Act, 1872. This relationship is neither hierarchical nor exclusive; rather, the statutes operate in overlapping and sometimes contradictory ways that prosecutors and courts must navigate case by case.

The Indian Penal Code continues to apply to cyber-enabled versions of traditional offences. Fraud committed through electronic means remains prosecutable under sections 420 and 468 IPC; defamation published online falls within section 499; criminal intimidation via electronic communication is addressed by section 506.

The Information Technology Act provides specialized offences for conduct uniquely enabled

[3] Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009).

by computer technology unauthorized access, data theft, system interference but many cybercrimes involve both IPC and IT Act violations, requiring prosecutors to determine charging strategy and courts to reconcile potentially different evidentiary and procedural requirements.

The Code of Criminal Procedure governs investigation and trial procedures, yet its provisions were designed for physical evidence and territorial crime. Search and seizure provisions under sections 93 to 98 CrPC contemplate physical premises and tangible objects; their application to data stored on remote servers, often in foreign jurisdictions, strains textual interpretation. The 2008 IT Act amendments introduced section 80, empowering police officers to enter and search public places for cybercrime investigation, but this provision addresses only a narrow category of investigative scenarios.

The Indian Evidence Act's treatment of electronic records, primarily through section 65B, represents the most doctrinally contested intersection. Section 65B, introduced by the Information Technology Act, 2000, establishes conditions for the admissibility of electronic records as evidence, requiring 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.[4]

The provision was intended to address authentication concerns specific to electronic evidence, its susceptibility to undetectable alteration, the complexity of computer systems, the need for technical expertise in verification. Yet judicial interpretation of section 65B has generated more confusion than clarity, as subsequent analysis demonstrates.

The Bharatiya Sakshya Adhiniyam, 2023, which replaces the Indian Evidence Act with effect from July 2024, substantially reproduces the section 65B framework in its section 63, suggesting legislative satisfaction with the existing approach despite persistent judicial and scholarly criticism.[5] This legislative continuity, in the face of documented doctrinal difficulties, reflects either considered judgment that the problems lie in interpretation rather than statutory design, or insufficient attention to the operational realities of cybercrime prosecution.

[4] Indian Evidence Act, 1872, s. 65B(4).
[5] Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023), s. 63.

2.3 Constitutional Dimensions

The constitutional framework within which cybercrime prosecution operates has been fundamentally reshaped by the Supreme Court's recognition of privacy as a fundamental right in *K.S. Puttaswamy v. Union of India*.[6] The nine-judge bench decision established that any state intrusion upon privacy must satisfy the requirements of legality, legitimate aim, and proportionality. This constitutional standard applies with particular force to digital investigations, which by their nature involve access to intimate personal information communications, lo- cation data, browsing history, financial records that collectively constitute what the Court termed the "informational privacy" dimension of article 21.

The tension between investigative necessity and privacy protection manifests acutely in cybercrime cases. Effective investigation often requires access to encrypted communications, real-time surveillance of network traffic, or preservation orders directed at service providers. Each such measure engages privacy interests that, post *Puttaswamy*, receive constitutional protection. Yet the statutory framework predates this constitutional development; the Information Technology Act's surveillance provisions, particularly sections 69 and 69A authorizing interception and blocking, were enacted without the proportionality framework that *Puttaswamy* now mandates.

The due process implications extend to the accused's rights in criminal proceedings. Article 21's guarantee against deprivation of life and liberty except by procedure established by law requires that evidentiary and procedural rules be applied consistently and fairly. When section 65B certification requirements oscillate between mandatory and discretionary depending on which Supreme Court decision is followed, the resulting uncertainty itself becomes a due process concern. Similarly, when jurisdictional assertions under section 75 permit prosecution of conduct occurring entirely abroad, questions arise regarding the adequacy of notice and the fairness of subjecting foreign actors to Indian criminal law.

3. Evidentiary Challenges in Cybercrime Prosecution

3.1 The Section 65B Certification Controversy

No provision of Indian evidence law has generated more judicial confusion than section 65B of the Indian Evidence Act, governing the admissibility of electronic records. The provision

[6] *K.S. Puttaswamy v. Union of India*, (2017) 10 SCC 1.

establishes that electronic records shall be admissible as evidence of their contents if the conditions specified in subsection (2) are satisfied conditions relating to the regular use of the computer, the regular feeding of information, the proper operation of the computer, and the accurate reproduction of information. Subsection (4) requires a certificate identifying the electronic record, describing the manner of its production, and providing particulars of the device involved, signed by a person occupying a responsible official position.

The Supreme Court's interpretation of these requirements has traced an erratic path. In *Anvar P.V. v. P.K. Basheer*,[7] a three-judge bench held that section 65B constitutes a complete code for the admissibility of electronic evidence, and that the certificate under section 65B(4) is a mandatory requirement that cannot be dispensed with. The Court explicitly overruled the earlier decision in *State (NCT of Delhi) v. Navjot Sandhu*,[8] which had suggested that electronic evidence could be proved through other means under sections 63 and 65 of the Evidence Act. The *Anvar* decision emphasized that electronic records are inherently susceptible to tampering and that the certification requirement provides essential safeguards for reliability.

The rigidity of *Anvar* produced practical difficulties that the Court subsequently attempted to address in *Shafhi Mohammad v. State of Himachal Pradesh*.[9] Here, a three-judge bench appeared to soften the mandatory certification requirement, holding that the applicability of procedural requirements under section 65B(4) would depend on whether the electronic evidence was produced by a person who was in a position to produce such certificate. The Court observed that requiring certification in all cases could defeat the very purpose of the provision, particularly where the electronic record was in the possession of the opposite party or a third party beyond the control of the person seeking to rely upon it.

The doctrinal tension between *Anvar* and *Shafhi Mohammad* required resolution, which the Supreme Court attempted in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*.[10] A three-judge bench reaffirmed the mandatory nature of the section 65B(4) certificate as established in *Anvar*, while clarifying that the requirement applies when a party seeks to produce electronic evidence that is not an original. The Court held that *Shafhi Mohammad* had

[7] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
[8] *State (NCT of Delhi) v. Navjot Sandhu*, (2005) 11 SCC 600.
[9] *Shafhi Mohammad v. State of Himachal Pradesh*, (2018) 2 SCC 801.
[10] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

been incorrectly decided to the extent it diluted the certification requirement, though it acknowledged that where the original electronic record is produced, no certificate is required. The decision also recognized that courts could permit the production of certificates at later stages of proceedings to prevent injustice.

Yet *Arjun Panditrao Khotkar* did not resolve all difficulties. The distinction between "original" electronic records and "copies" is itself technologically problematic. In digital systems, the concept of an "original" is often meaningless data exists as patterns of electrical charges or magnetic orientations that are constantly copied and moved within and between storage media. Every display of an electronic document involves copying from storage to memory to screen. The legal framework's reliance on concepts derived from documentary evidence originals, copies, duplicates maps imperfectly onto digital phenomena.

Moreover, the certification requirement places significant burdens on prosecutors and litigants. Obtaining a certificate from a person occupying a "responsible official position" in relation to the operation of a computer system may be straightforward when the evidence comes from a bank or government department, but becomes complicated when the evidence originates from personal devices, cloud services operated by foreign corporations, or systems administered by the accused. The requirement that the certifier have knowledge of the computer's operation, the regularity of information feeding, and the proper functioning of the system during the relevant period demands technical expertise that many potential certifiers lack.

3.2 Chain of Custody and Forensic Integrity

Beyond certification, the evidentiary integrity of electronic records depends upon establishing an unbroken chain of custody from seizure to courtroom presentation. Electronic evidence is uniquely vulnerable to alteration changes can be made without physical trace, timestamps can be manipulated, metadata can be modified or deleted. The legal system's response to this vulnerability has been to emphasize procedural safeguards: hash value verification, write-detailed documentation of handling, and testimony from qualified forensic examiners. blocking during forensic imaging,

Hash values fixed-length alphanumeric strings generated by cryptographic algorithms applied to data provide a mechanism for verifying that electronic evidence has not been altered since acquisition. Any modification to the underlying data, however minor, produces a different hash

value. Courts have increasingly recognized the evidentiary significance of hash verification, though the legal framework does not mandate specific forensic protocols. The absence of statutory standards means that the adequacy of forensic procedures is determined case by case, with courts possessing varying degrees of technical sophistication.

The institutional capacity for digital forensics in India remains inadequate to investigative demand. While the Central Forensic Science Laboratory and state forensic laboratories have established cyber forensic divisions, these facilities face backlogs, resource constraints, and challenges in maintaining technical currency as technologies evolve. The private forensic sector supplements government capacity but raises questions regarding accreditation, quality control, and the independence of expert testimony. Investigators without forensic training may compromise evidence through improper handling powering on seized devices, failing to document the seizure environment, or neglecting to preserve volatile data.

The problems are compounded in cases involving cloud-stored evidence. When data resides on servers operated by third parties, potentially in foreign jurisdictions, the chain of custody analysis must account for the service provider's data handling practices, the security of transmission, and the reliability of any copies produced in response to legal process. The party seeking to admit such evidence may have no direct knowledge of the systems involved and must rely upon the provider's representations re-presentations that may be challenged but are difficult to independently verify.

3.3 Digital Search and Seizure

The search and seizure of electronic evidence raises procedural questions that existing law addresses incompletely. The Code of Criminal Procedure's search provisions, drafted for physical premises and tangible objects, require adaptation to digital contexts where "searching" may mean examining data structures rather than physical spaces, and "seizing" may mean copying rather than removing.

Section 80 of the Information Technology Act empowers police officers not below the rank of Inspector to enter any public place and search and arrest without warrant any person reasonably suspected of having committed or being about to commit any offence under the Act. The provision's limitation to "public places" excludes private premises, where much cybercrime related evidence is located. For searches of private premises, investigators must rely upon CrPC

provisions section 93 for search warrants, section 165 for searches during investigation that do not specifically address the unique characteristics of digital evidence.

The scope of digital searches raises Fourth Amendment-analogous concerns under article 21. A search of a smartphone or computer potentially exposes the entirety of an individual's digital life communications, photographs, financial records, location history, browsing activity. The Supreme Court of the United States recognized in *Riley v. California*[11] that the search of a cell phone implicates privacy interests qualitatively different from the search of physical containers, warranting heightened procedural protection. Indian courts have not yet developed comparable jurisprudence specifically addressing digital search, though the *Puttaswamy* framework provides constitutional foundation for such development.

Cross-border data acquisition presents the most intractable procedural difficulties. When evidence resides on servers located outside India, investigators cannot simply execute search warrants; they must navigate international legal assistance mechanisms that are slow, cumber-some, and often unsuccessful. The Mutual Legal Assistance Treaty process may take months or years to produce results, if it produces results at all. Meanwhile, the evidence may be deleted, the suspect may flee, and the investigation may stall. Some investigators have responded by seeking to compel production from Indian subsidiaries or local representatives of foreign technology companies an approach that raises jurisdictional questions and has produced inconsistent judicial responses.

4. Jurisdictional Complexity and Extraterritorial Enforcement

4.1 Section 75 and the Territorial Nexus

Section 75 of the Information Technology Act provides that the Act shall apply to any offence or contravention committed outside India by any person if the act or conduct constituting the offence involves a computer, computer system, or computer network located in India.[12] This provision asserts extraterritorial jurisdiction based on the effects doctrine the principle that a state may exercise jurisdiction over conduct occurring abroad that produces effects within its territory. The provision is notable for its breadth; it does not require that the offender be an Indian national, that the victim be Indian, or that the primary conduct occur in India. The sole

[11] *Riley v. California*, 573 U.S. 373 (2014).
[12] Information Technology Act, 2000, s. 75.

nexus required is that the offence "involve" a computer located in India.

The interpretive difficulties with section 75 are substantial. The term "involves" is undefined and could be construed narrowly to require that the Indian computer be integral to the offence, or broadly to encompass any incidental connection. A phishing email sent from abroad to an Indian recipient "involves" the recipient's computer, but so might a denial-of-service attack that routes traffic through Indian servers as part of a botnet targeting systems elsewhere. The statutory language provides no guidance for distinguishing cases where Indian jurisdiction is appropriate from cases where the Indian connection is too attenuated to justify prosecution.

Moreover, the assertion of jurisdiction does not ensure the capacity for enforcement. Section 75 may authorize Indian courts to try offences committed abroad, but it cannot compel foreign suspects to appear, cannot execute search warrants on foreign soil, and cannot seize assets beyond Indian territorial reach. The provision thus creates a gap between jurisdictional authority and practical enforceability a gap that is particularly pronounced for cybercrimes committed by sophisticated actors who deliberately structure their activities to avoid jurisdictions capable of effective prosecution.

4.2 Mutual Legal Assistance and International Cooperation

The enforcement gap that section 75 cannot bridge must be addressed through international cooperation mechanisms, primarily Mutual Legal Assistance Treaties. India has entered into MLATs with numerous countries, and the Code of Criminal Procedure provides domestic procedures for executing foreign requests and transmitting Indian requests abroad.[13] Yet the MLAT process is widely acknowledged to be inadequate for the speed and volume of cyber-crime investigations.

The structural limitations are inherent to the treaty mechanism. MLAT requests must be transmitted through central authorities typically the Ministry of Home Affairs in India and the Department of Justice in the United States adding bureaucratic layers to each request. The requested state must evaluate the request against its own legal standards, which may differ from those of the requesting state. Dual criminality requirements may prevent assistance where

[13] Code of Criminal Procedure, 1973, Chapter VIIA (ss. 166A–166B), as by the Code of Criminal Procedure (Amendment) Act, 2005.

the conduct, though criminal in the requesting state, is not criminal in the requested state. Even when requests are approved, execution depends upon the requested state's investigative resources and priorities.

For cybercrime investigations, these delays are often fatal to effective prosecution. Electronic evidence may be retained by service providers for limited periods often 90 to 180 days after which it is deleted pursuant to data minimization policies. An MLAT request that takes twelve months to process will frequently find that the sought evidence no longer exists. Sophisticated criminals are aware of these limitations and structure their activities accordingly, using services with minimal retention policies, jurisdictions with limited cooperation, and technical measures that complicate attribution.

India is not a party to the Budapest Convention on Cybercrime, the primary international instrument facilitating cooperation in cybercrime investigations.[14] The Convention establishes expedited preservation mechanisms, direct communication between law enforcement authorities, and harmonized procedural standards that significantly accelerate cross-border evidence gathering. India's non-participation reportedly due to concerns about sovereignty and the Convention's origins in a European institution excludes Indian investigators from these streamlined procedures and limits cooperation with the Convention's numerous state parties.

4.3 Anonymization, Encryption, and the Dark Web

Technical barriers compound the legal obstacles to transnational cybercrime investigation. The proliferation of anonymization technologies Tor, virtual private networks, proxy chains enables offenders to obscure their identities and locations, frustrating attribution efforts even when jurisdiction could theoretically be established. The dark web, accessible only through anonymizing browsers, hosts marketplaces for illegal goods and services, forums for criminal coordination, and infrastructure for cyberattacks, all operating beyond the reach of conventional investigative techniques.

Encryption presents a distinct but related challenge. End-to-end encrypted communications, increasingly the default for messaging applications, cannot be intercepted in intelligible form even with lawful authorization. Device encryption may render seized computers and

[14] Convention on Cybercrime (adopted November 23, 2001) E.T.S. No. 185.

smartphones inaccessible without the cooperation of the user or the exploitation of security vulnerabilities. The tension between law enforcement's investigative needs and the security benefits of strong encryption has produced intense policy debate globally, with no consensus resolution.

Indian law provides limited tools for addressing these technical barriers. Section 69 of the Information Technology Act authorizes the government to direct interception of information, but this authority is ineffective against properly implemented end-to-end encryption where the service provider does not possess decryption keys.[15] The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009, contemplate decryption orders, but compelling decryption from uncooperative foreign providers or individual users raises both practical and constitutional difficulties.

4.4 Platform Immunity and Intermediary Liability

The role of intermediaries internet service providers, social media platforms, messaging services, cloud storage providers in cybercrime investigation implicates the liability framework established by section 79 of the Information Technology Act. Section 79 provides conditional immunity to intermediaries for third-party content, subject to compliance with due diligence requirements and response to government directions for content removal.[16] The provision, as per the Supreme Court in *Shreya Singhal v. Union of India*,[17] requires actual knowledge of specific illegal content before intermediary liability attaches.

For investigative purposes, the intermediary liability framework interacts with obligations to preserve and produce evidence. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, impose requirements including traceability of the "first originator" of information for significant social media intermediaries a requirement that has been challenged as incompatible with end-to-end encryption and that implicates privacy concerns.[18] The constitutional validity of these requirements remains under judicial consideration.

[15] Information Technology Act, 2000, s. 69.
[16] Information Technology Act, 2000, s. 79.
[17] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1.
[18] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 4(2).

Enforcement against multinational technology corporations presents particular difficulties. These entities may have minimal physical presence in India while providing services to hundreds of millions of Indian users. Compelling compliance with Indian legal process requires either effective extraterritorial jurisdiction which, as discussed, is limited or cooperation mechanisms that the corporations may resist on legal, technical, or policy grounds. The data localization debate, concerning requirements that certain data be stored within India, represents one regulatory response to these enforcement challenges, though localization mandates raise their own concerns regarding internet fragmentation and economic efficiency.

5. Comparative Jurisprudence

5.1 United States: The Computer Fraud and Abuse Act

The United States Computer Fraud and Abuse Act (CFAA), enacted in 1986 and subsequently amended, provides the primary federal statute for computer crime prosecution.[19] The CFAA criminalizes unauthorized access to computers, exceeding authorized access, trafficking in passwords, and various forms of computer-enabled fraud and damage. The statute's interpretation has been contested, particularly regarding the meaning of "exceeds authorized access" a question the Supreme Court addressed in *Van Buren v. United States*,[20] adopting a narrow construction that limits criminal liability to accessing information one is not entitled to obtain, rather than misusing information one is entitled to access.

For evidentiary purposes, the United States Federal Rules of Evidence do not impose certification requirements analogous to section 65B. Electronic evidence is subject to general authentication requirements under Rule 901, which permits authentication through testimony of a witness with knowledge, distinctive characteristics, or other methods. The absence of a specific electronic evidence certification regime reflects a different legislative judgment that general evidentiary principles, combined with judicial discretion and adversarial testing, adequately address reliability concerns.

The U.S. approach to cross-border evidence gathering has evolved significantly with the Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018,[21] which authorizes U.S. law enforcement to compel production of data from U.S.-based providers regardless of where the

[19] 18 U.S.C. s. 1030 (2023).
[20] *Van Buren v. United States*, 141 S. Ct. 1648 (2021).
[21] Clarifying Lawful Overseas Use of Data Act, Pub. L. No. 115-141, 132 Stat. 1213 (2018).

data is stored, while establishing a framework for executive agreements with foreign governments to facilitate reciprocal access. The CLOUD Act represents a departure from traditional MLAT-based cooperation, enabling direct requests to providers subject to comity-based objection procedures. India has engaged in discussions regarding a CLOUD Act executive agreement, though no agreement has yet been concluded.

5.2 United Kingdom: The Computer Misuse Act

The United Kingdom Computer Misuse Act 1990, as amended, establishes offences of unauthorized access to computer material, unauthorized access with intent to commit further offences, and unauthorized acts with intent to impair computer operation.[22] The Act has been updated to address contemporary threats, including the Serious Crime Act 2015 amendments creating an offence of unauthorized acts causing serious damage.

The UK evidentiary framework, like the US approach, does not impose certification requirements comparable to section 65B. The Police & Criminal Evidence Act 1984 and the Civil Evidence Act 1995 address electronic evidence through general provisions on documentary evidence and hearsay, supplemented by common law authentication requirements. Courts assess reliability through the adversarial process rather than mandatory certification.

The UK's participation in the Budapest Convention facilitates cross-border cooperation through expedited preservation requests, direct law enforcement communication, and harmonized procedural standards. Post-Brexit arrangements have required renegotiation of cooperation mechanisms with EU member states, but the UK remains committed to the Convention framework and has concluded bilateral agreements to maintain investigative cooperation.

5.3 The Budapest Convention Framework

The Budapest Convention on Cybercrime, opened for signature in 2001, represents the most significant international effort to harmonize cybercrime law and facilitate cross-border cooperation.[23] The Convention establishes minimum standards in relation to substantive

[22] Computer Misuse Act 1990 (UK), c. 18.
[23] Id. The Convention has been ratified by 68 states as of 2024, including non-Council of Europe members such as the United States, Japan, and Australia.

criminal provisions in cyberspace, procedural tools for investigation, and international coordination systems.

The Convention's procedural provisions are particularly relevant to the difficulties facing Indian investigators. Article 29 establishes expedited preservation of stored computer data, enabling requesting states to secure evidence preservation pending formal MLAT requests. Article 35 establishes a 24/7 network of contact points for immediate assistance in cybercrime in- vestigations. These mechanisms significantly accelerate cross-border evidence gathering com- pared to traditional MLAT procedures.

India's non-participation in the Budapest Convention reflects policy concerns regarding the Convention's negotiation process, which did not include India, and provisions that some view as insufficiently protective of sovereignty. However, non-participation imposes costs in terms of investigative cooperation and excludes India from the Convention's ongoing development, including the Second Additional Protocol on Enhanced International Cooperation, which fur- ther streamlines evidence gathering procedures.[24]

6. Institutional and Doctrinal Critique

6.1 Statutory Ambiguity and Legislative Inertia

The foregoing analysis reveals pervasive statutory ambiguity in the legal framework governing cybercrime prosecution. Section 65B's certification requirements, section 75's jurisdictional nexus, the scope of intermediary obligations, and the procedures for cross-border evidence gathering all suffer from drafting that fails to provide clear guidance for application. This ambiguity is not merely a technical deficiency; it transfers decision-making authority from the legislature to the judiciary, producing case-by-case determinations that may lack consistency and predictability.

The legislature has demonstrated limited responsiveness to these difficulties. The 2008 amendments to the Information Technology Act, while expanding substantive offences, did not address the procedural and evidentiary challenges that had already become apparent. The Bharatiya Sakshya Adhiniyam, 2023, reproduces the section 65B framework despite two decades

[24] Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (adopted May 12, 2022) C.E.T.S. No. 224.

of interpretive difficulty. Proposed amendments to address specific problems such as the Law Commission's recommendations regarding electronic evidence have not been enacted.[25] This legislative inertia leaves courts to manage doctrinal difficulties through interpretation, a process that has produced the oscillation documented above.

6.2 Judicial Oscillation and Doctrinal Instability

The Supreme Court's treatment of section 65B exemplifies a broader pattern of doctrinal instability in cybercrime jurisprudence. The progression from *Navjot Sandhu* through *Anvar*, *Shafhi Mohammad*, and *Arjun Panditrao Khotkar* reflects not incremental refinement but fundamental disagreement about the proper interpretation of statutory requirements. Three-judge benches have overruled or distinguished prior three-judge bench decisions, producing a jurisprudence that practitioners struggle to apply with confidence.

This instability has practical consequences. Prosecutors must anticipate which interpretive approach a particular court will follow, potentially tailoring evidence presentation strategies to judicial preferences rather than statutory requirements. Defence counsel can challenge electronic evidence on procedural grounds that may or may not succeed depending on the panel. Trial courts must navigate conflicting appellate guidance, sometimes producing inconsistent outcomes on similar facts. The resulting uncertainty undermines the rule of law values that consistent legal standards are meant to serve.

6.3 Institutional Capacity Deficits

Effective cybercrime prosecution requires institutional capacities that the Indian criminal justice system has not adequately developed. Investigating officers often lack technical training to understand digital evidence, preserve it properly, and present it effectively. Prosecutors may be unfamiliar with the technical concepts necessary to establish chain of custody and authenticate electronic records. Judges may lack the background to evaluate expert testimony critically or to assess the reliability of forensic methodologies.

Forensic laboratory capacity is insufficient for investigative demand. The absence of standardized protocols means that forensic practices vary across laboratories and examiners, complicating quality assessment and creating opportunities for defence challenge.

[25] Law Commission of India, *185th Report on Review of the Indian Evidence Act, 1872* (2003).

Accreditation mechanisms exist but are not uniformly applied. The result is a forensic infrastructure that cannot consistently support the evidentiary requirements of cybercrime prosecution.

Specialized cyber police stations and cybercrime cells have been established in various states, but their effectiveness varies considerably. Coordination between state police and central agencies the Central Bureau of Investigation, National Investigation Agency, and specialized units is often inadequate for complex investigations spanning multiple jurisdictions. The federal structure of Indian policing, with law enforcement primarily a state subject, complicates the coordinated response that transnational cybercrime requires.

6.4 Privacy, Prosecution, and Constitutional Proportionality

The constitutional framework established by *Puttaswamy* requires that investigative measures intruding upon privacy satisfy requirements of legality, legitimate aim, and proportionality.[26] The existing statutory framework for cybercrime investigation was enacted before this constitutional development and has not been systematically evaluated against the proportionality standard.

Several provisions raise proportionality concerns. Section 69's interception authority, while subject to procedural safeguards under the 2009 Rules, permits surveillance that may be broader than necessary for legitimate investigative purposes. The traceability requirement for messaging platforms under the 2021 Intermediary Rules, if implemented, would compromise the security benefits of end-to-end encryption for all users to facilitate investigation of a small number of offenders. Bulk data preservation requirements impose costs on service providers and create databases that, if breached, would expose sensitive personal information.

The proportionality analysis requires balancing investigative necessity against privacy intrusion a balance that may differ across offence categories, evidence types, and investigative stages. Serious cybercrimes threatening national security or involving exploitation of children may justify more intrusive measures than minor offences. Real-time interception may require higher justification than access to stored communications. Emergency circumstances may warrant expedited procedures that would be inappropriate for routine investigations. The

[26] *K.S. Puttaswamy*, supra note 5.

current statutory framework does not adequately differentiate among these contexts, applying uniform standards that may be either over-inclusive or under-inclusive depending on the circumstances.

7. Reform Proposals

The deficiencies identified in this analysis require legislative and institutional responses that address both specific doctrinal problems and systemic capacity limitations. The following proposals are offered as legally viable reforms grounded in comparative experience and constitutional requirements.

7.1 Section 65B Reform

The certification requirement under section 65B should be reformulated to focus on reliability rather than formal compliance. The current framework privileges certification by a person in a "responsible official position" without ensuring that the certifier possesses the technical knowledge necessary to verify the conditions specified in section 65B(2). Reform should establish tiered requirements calibrated to the complexity of the electronic evidence and the availability of certification.

For evidence from institutional sources banks, government departments, established corporation's certification by a designated officer with specified technical qualifications should remain appropriate. For evidence from personal devices or small entities, alternative authentication mechanisms should be permitted, including testimony from forensic examiners who have analyzed the evidence, hash value verification demonstrating integrity, and metadata analysis establishing provenance. For evidence obtained from third-party service providers, the provider's business records certification, combined with forensic verification of the produced data, should suffice.

The distinction between "original" and "copy" electronic records should be abandoned as technologically incoherent. All electronic evidence should be subject to authentication requirements focused on reliability whether the evidence accurately represents the data it purports to represent and whether that data has been preserved without material alteration. This functional approach would align Indian law with international practice and eliminate the conceptual confusion that has characterized section 65B jurisprudence.

7.2 Standardized Forensic Protocols

Legislative or regulatory establishment of mandatory forensic protocols for digital evidence handling would address the current inconsistency in investigative practices. These protocols should specify requirements for evidence seizure, imaging, storage, analysis, and presentation, drawing upon international standards such as those developed by the Scientific Working Group on Digital Evidence and the International Organization on Computer Evidence.

Key protocol elements should include: mandatory hash value generation at acquisition; write-blocking during forensic imaging; documented chain of custody with time stamped transfers; analysis on forensic copies rather than original media; standardized reporting formats for forensic findings; and qualification requirements for forensic examiners. Compliance with these protocols should create a presumption of integrity that shifts the burden to the challenging party to demonstrate specific grounds for questioning the evidence.

Forensic laboratory accreditation should be mandatory for laboratories whose findings are admitted in court. The National Accreditation Board for Testing and Calibration Laboratories (NABL) or a specialized body should establish accreditation standards for digital forensic laboratories, with regular audits and proficiency testing. Accreditation status should be disclosed in forensic reports and considered by courts in evaluating expert testimony.

7.3 Specialized Cyber Adjudicatory Mechanisms

The technical complexity of cybercrime cases warrants specialized adjudicatory mechanisms with enhanced technical capacity. Dedicated cybercrime courts, staffed by judges with technical training and supported by court-appointed technical experts, would improve the quality of adjudication and reduce the inconsistency that results from generalist judges applying unfamiliar technical concepts.

The existing Adjudicating Officer mechanism under section 46 of the Information Technology Act, with jurisdiction over contraventions attracting civil penalties, provides a partial model. Expansion of this model to criminal matters, with appropriate procedural safeguards, would create specialized forums for cybercrime prosecution. Alternatively, designated sessions courts with cybercrime jurisdiction, supported by technical assessors, could address the need for specialized adjudication within the existing court structure.

Judicial training programs should be expanded and institutionalized. The National Judicial Academy and state judicial academies should offer regular programs on digital evidence, cybercrime investigation, and emerging technologies. Judicial officers assigned to cybercrime matters should be required to complete specified training before assuming such assignments.

7.4 International Cooperation Enhancement

India should reassess its current position regarding the Budapest Convention. The concerns that motivated non-participation sovereignty, negotiation process, European origins must be weighed against the practical benefits of Convention membership for Indian investigators and the costs of exclusion from the primary international framework for cybercrime cooperation. Observer status, available under the Convention, would permit participation in Committee of Parties de- liberations without full ratification, enabling India to influence the Convention's development while assessing the implications of full membership. Pending any decision on the Budapest Convention, India should pursue bilateral agreements that establish expedited cooperation mechanisms for cybercrime investigations. The CLOUD Act executive agreement framework offers a model for direct law enforcement access to data held by providers, bypassing traditional MLAT delays. Agreements with major technology company home jurisdictions the United States, Ireland, Singapore would address a significant proportion of cross-border evidence needs.

Domestic legal process for international evidence requests should be streamlined. Dedicated units within the Ministry of Home Affairs and Ministry of External Affairs should handle cybercrime-related MLAT requests with priority processing. Template requests for common evidence types would reduce preparation time. Electronic transmission of requests and responses, where treaty partners permit, would accelerate the process.

7.5 Constitutional Calibration

The investigative framework should be recalibrated to satisfy *Puttaswamy* proportionality requirements. This requires differentiated authorization procedures based on the intrusiveness of the investigative measure and the seriousness of the offence under investigation. Real time interception should require judicial authorization with specified findings regarding necessity and proportionality. Access to stored communications should require authorization calibrated to the sensitivity of the content and the period covered. Metadata access, while less intrusive than content access, should nonetheless require legal process with documented justification.

Oversight mechanisms should be strengthened. The review committee established under section 69 should be reconstituted with greater independence and enhanced powers. Regular reporting on surveillance authorizations, with appropriate classification protections, would enable legislative oversight. An independent inspector or ombudsman for digital surveillance, modeled on similar institutions in other democracies, would provide ongoing scrutiny of investigative practices.

8. Conclusion

The prosecution of cybercrime in India operates within a legal framework that has not kept pace with technological transformation or doctrinal development. The evidentiary regime for electronic records, centered on section 65B certification requirements, has produced judicial confusion rather than reliable standards, with the Supreme Court's interpretive oscillation undermining the consistency that criminal adjudication requires. The jurisdictional framework, while asserting expansive extraterritorial authority under section 75, cannot translate that assertion into effective enforcement against transnational offenders beyond Indian territorial reach. Institutional capacities investigative, forensic, judicial remain inadequate to the technical demands of digital crime.

These deficiencies are not merely administrative inconveniences; they compromise the fundamental objectives of criminal law. When reliable electronic evidence is excluded on procedural technicalities unrelated to its accuracy, guilty offenders may escape accountability. When jurisdictional limitations prevent investigation of crimes victimizing Indian citizens, the protective function of criminal law fails. When privacy-invasive investigative measures proceed without proportionality constraints, constitutional rights suffer. The current framework produces these failures with troubling regularity.

Reform is both necessary and achievable. The proposals advanced in this article, reformulation of section 65B to emphasize reliability over formal certification, establishment of standardized forensic protocols, creation of specialized cyber adjudicatory mechanisms, enhancement of international cooperation, and constitutional calibration of investigative powers are legally viable and practically implementable. They draw upon comparative experience demonstrating that effective cybercrime prosecution can coexist with rights protection, and they respond to the specific doctrinal difficulties that Indian courts have identified.

The urgency of reform increases as cybercrime continues to escalate in volume and sophistication. Each year of legislative inertia compounds the enforcement deficit and normalizes doctrinal incoherence. The digital transformation of Indian society accelerated by initiatives promoting digital payments, e-governance, and online services expands the attack surface for cybercriminals while increasing the stakes of effective prosecution. A legal framework designed for an earlier technological era cannot adequately protect a society that has moved decisively into the digital age.

The path forward requires recognition that cybercrime prosecution presents distinctive challenges warranting distinctive legal responses. The transplantation of concepts from physical evidence law to digital contexts has produced the interpretive difficulties documented throughout this analysis. Effective reform must begin from technological realities rather than legal analogies, constructing frameworks that accurately reflect how digital systems operate and how electronic evidence can be reliably authenticated. This is not a call for abandoning traditional legal values due process, proportionality, the presumption of innocence but for expressing those values through mechanisms appropriate to the digital environment.

The legitimacy of criminal adjudication depends upon the capacity to determine guilt and innocence accurately, fairly, and consistently. When evidentiary rules exclude reliable evidence or admit unreliable evidence, when jurisdictional frameworks assert authority they cannot exercise, when investigative powers operate without constitutional constraint, that legitimacy is compromised. The reforms proposed here aim to restore coherence to a framework that has lost it, enabling the criminal justice system to fulfill its essential functions in an era when crime, like so much else, has migrated to digital spaces.