CLICK, COMMIT, CONVICT: EVIDENTIARY CHALLENGES IN PROSECUTION OF CYBERCRIME

Nisha Verma, LLM, CUSB, Gaya

Dr. Deo Narayan Singh, Assistant Professor, CUSB, Gaya

ABSTRACT

The digital revolution drastically changed international social and economic relations, but also increased chances for cybercriminals. Inspite of legislative paradigms such as the Information Technology Act, 2000, Budapest Convention, 2001, the rate of conviction in India for cybercrime is less than two percent (2020–2023), mainly because of procedural and evidence failures. It posses that volatility of digital evidence, absence of forensic capability, and cross-border jurisdictional difficulties undermine convictions. The accelerated growth of digital technology affected human behaviors as well as increased the opportunity for cybercriminals. In the technological surge, cybercriminals are able to take advantage of cyberspace through different ways such as fraud, identity theft, ransomware and cyberterrorism. Despite increase in incidents, conviction rate remain alarmingly low, as illustrated by India's 0-2 % conviction rate between 2020 and 2022. This research article utilizes doctrinal and comparative analysis in assessing technical, procedural, and jurisdictional loopholes in prosecuting cyber offences under the Bharatiya Nyaya Sanhita (BNS), 2023 and Bharatiya Shakshya Adhinayam (BSA), 2023, Information and Technology Act, 2000. The study is a review article of evidentiary and jurisdictional challenges that impede successful conviction of cybercriminals. The review article centers around definitional ambiguities of cybercrime, the instability and complexity of digital evidence, and the transnational nature of offence that makes adjudication and enforcement difficult. The prosecution of cybercrime is greatly inhibited by issues like, encryption, anonymization, a fragile chain of custody, lack or disparities in technical expertise, and ineffective forensic capacity. Jurisdictional dilemmas, demonstrated through Indian case laws and application of international treaties, such as the Budapest Convention 2001, would benefit from standardized international legal norms and enhanced institutional cooperation. According to the article, successful responses necessitate a multifaceted strategy that combines capacity building, legal reforms, technological innovation, and cross-border cooperation to guarantee that cybercriminals who "click and commit" are eventually found guilty. The research ends with suggestions to harmonize procedures for digital evidence with international standards like the Budapest

Convention, 2001 and to enhance inter-agency coordination through technological and institutional reforms.

Keywords: Cybercrime, Cross-border jurisdiction, definitional ambiguities, Information Technology Act, 2000, Bharatiya Nyaya Sanhita (BNS), 2023, Bharatiya Sakshya Adhiniyam (BSA), 2023, Budapest Convention on Cybercrime 2001, Technological innovation.

Introduction

Speedy growth of digital technology completely changed the way of living, working, interacting and also opened the doors for cyber criminals to misuse these technologies. Digital revolution has transformed criminal activities where cybercriminals can just click, commit, and potentially evade conviction, due to significant challenges faced in their prosecution. As per the data of a newspaper article it is found that 1.67 lakh cybercrime cases have been registered during 20202022 in 28 Indian states,only 1.6% of these criminals were convicted[1]. As per the data of NCRB, maximum number of cases were registered in Uttar Pradesh and Karnataka between 2020-2022, and the rate of conviction was 0 -2 %. The study reports a high gap between digital criminal activities and their prosecution. Anonymization techniques, encryption issues, the dynamic and transient nature of digital evidence, and common failures to maintain an uninterrupted chain of custody make the evidence process in cybercrime extremely complex. Furthermore, current laws like the Information Technology Act of 2000 makes prosecution impossible due to ambiguous legal definitions of cybercrime and jurisdictional concerns. Legislative changes in recent years (i.e. the Bharatiya Nyaya Sanhita (BNS), 2023, and the

Bharatiya Sakshya Adhiniyam (BSA), 2023) regarding amendments to both the criminal and evidence laws have underscored the need for not just greater forensic and investigative capabilities, but also for clarity in terms of procedure and jurisdiction.

Specifically referenced in this article is the concept of "click, commit, convict" - the journey from a digital crime to accountability before a court - as a lens through which we may critically assess the numerous complex problems that law enforcement encounters in the prosecution of

[1] Animesh Singh, "Only 1.6% Conviction Rate in 2yrs Amid Surge in Cybercrime Cases", The Tribune (New Delhi, Dec. 24, 2024).
Available at: https://www.tribuneindia.com/news/india/only-1-6-conviction-rate-in-2-yrs-amid-surge-in-cybercrimecases-2/amp (last visited on September 18, 2025)

cyber crime.

The research attempts to outline workable reform and cooperative strategies to close the enforcement gap for India's digital criminal justice by looking at definitional ambiguity, procedural barriers, and jurisdictional issues.

The phrase "click, commit, convict" which charts the path from virtual offense to judicial responsibility is the subject of this article's critical analysis of the multifaceted difficulties faced by enforcement agencies when prosecuting cybercrime. The study attempts to provide workable reforms and collaborative strategies to bridge the enforcement gap for India's digital criminal justice by addressing jurisdictional issues, procedural obstacles, and definitional ambiguity.

Literature Review

The literature review establishes that Cybercrime is increasing rapidly in India and has consequences for the country's economy, national security, and public trust. Existing laws, particularly the Information Technology Act 2000, is antiquated and not adequate for mitigating the new range of cybercrime; for example, threats of ransomware, identity theft, and cyberterrorism. The legal framework is disjointed and challenges to address include jurisdictional issues, no standard definition, procedural issues, and lack of coordination between different investigative bodies.These challenges impede real investigation, prosecution, or deterrent to cybercrime. The review indicates comprehensive legal reforms, responsive to technology, are immediate, alongside building better coordination and capacity between the enforcement bodies[2].

Technology evolving rapidly as a growing strain on legal and forensic systems to keep evidentiary methods up to date with the increasing complexity of cybercrime.[3] Jurisdictional complexity in international cybercrime is also a factor in this on going development and makes collaboration and evidence gathering more difficult for international law enforcement

[2] Abeer Rakesh Wasnik, "Uncovering the legal challenges of Cybercrime in India and the need for a specific legal framework" *Journal of Legal Research and Juridical Sciences*, vol. 5(3) [2023] < https://jlrjs.com/wpcontent/uploads/2023/06/159.-Abeer-Wasnik.pdf> Accessed September 13, 2025

[3] Nischal Soni, " Digital Forensics: Confronting Modern Cyber Crimes, Technological Advancements, and Future Challenges" *Journal of Forensic Legal & Investigative Sciences,* [2025] < https://www.heraldopenaccess.us/openaccess/digital-forensics-confronting-modern-cyber-crimes-technologicaladvancements-and-future-challenges> Accessed September 13, 2025

agencies.[4] Technology complications such as evidence stored on multiple heterogeneous devices or in cloud computing environments complicate the collection of reliable and admissible evidence.[5]

The literature is generally in agreement that in order to establish effective legal frameworks and standard evidentiary protocols it requires collaboration of technical professionals and legal practitioners to address these challenges. Collaboration must be guided by a shared commitment to ensure reliability and legal admissibility of digital evidence when tested in a court of law.[6]

Among the key recommendations are the creation of standardized chain of custody protocols, updated legal standards to adapt to emerging technologies, and enhanced cyber forensic training for law enforcement officers.[7]

Studies also underscores the utmost necessity of correctly balancing successful prosecution of cybercrime against one's right to privacy, specifically in relation to legal protections, such as obtaining proper warrants, and unobstructed oversight into the online investigative process.

While the promise of improvement through forensic tools and collaboration globally may be encouraging, the literature encourages ongoing reforms to align evidence protocols with the state of the art of the threat posed by cyber criminals to pursue justice[8].

This discussion provides the foundation for examining indepth issues of evidence and providing solutions for improving the class of evidence utilized in prosecuting cyber crime in

---

[4] Anshu Kumar, "Cybercrime And Jurisdictional Challenges In International Criminal Law," 3 *International Journal of Law, Social Science and Security Studies* 356 (2025)< https://ijlsss.com/cybercrime-and-jurisdictional-challengesin-international-criminal-law/> Accessed September 13, 2025

[5] Moses Ashawa et al, "Digital Forensics Challenges in Cyberspace: Overcoming Legitimacy and Privacy Issues Through Modularisation," 5 *Cybersecurity and Digital Forensics Studies* 23 (2023) < https://ojs.wiserpub.com/index.php/CCDS/article/view/3845> Accessed on September 13, 2025

[6] P. Ganguli, "Admissibility of Digital Evidence under Bharatiya Sakshya Adhiniyam: Challenges and Legal Framework," 16 *International Journal of Law and Technology* 102 (2024) <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4977238> Accessed on September 13, 2025

[7] L. K. Saini, "10 Best Practices for Digital Evidence Collection," 8 *International Journal of Digital Forensics & Cyber Security* 210 (2025) <https://cellebrite.com/en/10-best-practices-for-digital-evidence-collection/> Accessed on September 13, 2025

[8] Ankit Kumar Yadav, "Balancing Privacy and Security: Constitutional Implications in the Era of Cyber Crime," *Indian Journal of Integrated Research in Law* (2025) Volume V Issue II | ISSN: 2583-0538<https://ijirl.com/wpcontent/uploads/2025/04/BALANCING-PRIVACY-AND-SECURITY-CONSTITUTIONAL-IMPLICATIONS-INTHE-ERA-OF-CYBER-CRIME.pdf > Accessed on September 14, 2025

the remaining sections of this research article.

The prosecution of cybercrime in India is faced with challenges on multiple fronts as noted by the most Recent literature on cybercrime and evidence. There is general consensus by the researchers that on the rapid and unprecedented development of digital technology has outpaced and plans to address some of that framework for dealing with cyber crimes. Wasnik (2023), emphasizes significant loophole issues within the Indian specified cyber crime laws noting that the Information Technology Act, constitutes an outdated and improper response to wonders such as ransomware issues, identity theft, cyberterrorism and the incapacitating nature of stalking[9]. The enactment of the Bharatiya Nyaya Sanhita and Bharatiya Sakshya Adhiniyam during 2023 to address cyber crime addresses concerns but proves unfocused regarding the procedural and enforcement recruitment capacity as relative to technological realities (Wasnik, 2023).[10]

Some major hindrances enumerated are the fickleness and complexity of digital evidence, which necessitates the use of specific forensic abilities and equipment available in India at present (Yadav and Tanwar, 2025)[11]. The transitory nature of electronic information combined with encryption and anonymization technology makes evidence retention and admissibility difficult, resulting in tenuous prosecution cases[12]. Vanita (2025) also points to jurisdictional difficulties brought about by the borderless nature of cybercrime, where crimes cross national borders, requiring harmonized global cooperation which India continues to develop (Vanita, 2025)[13].

Coordination and capacity-building challenges also afflict Indian cybercrime enforcement. Overlapping functions of various agencies, lack of skills, and underreporting crimes for fear of reputation further aggravate the dreadful conviction rate of around 1.6% during 2020-2023[14].

---

[9] Supra note 3
[10] Supra note 3
[11] Deewanshu Yadav and Sushma Tanwar, "Legal Challenges in Combating Cyber Crimes: A Critical Analysis," (2025) *International journal of Law and Legal Research*, ISSN : 2582- 8878 < https://www.ijllr.com/post/legalchallenges-in-combating-cyber-crimes-a-critical-analysis> Accessed on September 20, 2025
[12] Ram Prakash Chaubey, "Cybercrime Investigation in India: An Analysis of Digital Evidence and Its Role in Proving Cybercrimes," (2025) 7(3) *International Journal of Law, Policy and Social Review* 25–31, available at <https://www.lawjournals.net/assets/archives/2025/vol7issue3/7067.pdf> Accessed on September 20, 2025
[13] Vanita, "Jurisdictional Challenges in Cyber Crime Prosecution," 7 *Indian Journal of Law and Legal Research,* ISSN : 2582-8878 < https://www.ijllr.com/post/jurisdictional-challenges-in-cyber-crime-prosecution> Accessed on September 20, 2025
[14] LawPret, "Cyber Crime in India: A Comprehensive Report," (2025),< https://www.lawpret.com/cyber-crime-inindia-a-comprehensive-report/> Accessed on September 20, 2025

The literature emphasizes the need for immediate technological upgradation, extensive training of the judiciary and law enforcement, and rationalized legal procedures conforming to international norms like the Budapest Convention.[15]

In comparison, research proves that countries such as the EU, United States of America, and Singapore offer models of embracing superior forensic capacity and police collaboration that India can follow to maximize its prosecutorial efficiency (Yadav and Tanwar, 2025)[16]. Additionally, public-private partnerships and awareness campaigns are a determinant factor in early reporting and detection of cybercrime, creating a stronger enforcement system.

Overall, the literature review meets at the point of imperative for multi-faceted reforms legal, technological, institutional, and international addressing the enduring gap between increasing cases of cybercrime and India's ability to prosecute effectively. This review of literature offers a point of departure for examining India's prosecution challenges presently under the recent legislative developments and illuminating avenues for reform.

Origin, Nature and Scope

The literature review established that the term “cybercrime” was first coined by Sussman and Heutson in 1995. “Cybercrime can not be described in a single definition it is best considered as collection of acts or conducts – these acts are based on the material offence object and modus operandi that affect computer data or system”. The research provides that cybercrime covers two categories: crime where computer is object and where computer is used as tool.[17]

The nature of cybercrime is complex and has evolved with the emergence of digital technologies. The tools, platforms and process involved are intangible and have no geographical limits,which makes it borderless in nature. Illegal activities like stealing data, gaining financial advantages through phishing, malware, ransomware, online fraud, cyber

[15] Rakshita Mathur, “An In-Depth Study of the Budapest Convention on Cybercrime,” 2 *Cyber Law Reporter* 43 (2023) < https://thelawbrigade.com/wp-content/uploads/2023/12/Rakshita-Mathur-CYLR.pdf> Accessed on September 20, 2025

[16] Supra note 11

[17] Regner Sabillon, Jeimy Cano et al. , “Cybercrime and Cybercriminals: A comprehensive Study”, [2016] *International Journal of Computer Networks and Communications Security* Vol. 4, No.6, 165-176, ISSN 2410-0595 <https://www.researchgate.net/publication/304822458_Cybercrime_and_Cybercriminals_A_Comprehensive_Study > Accessed on September 20, 2025

terrorism harassment etc. are included under cybercrime.

The scope of cybercrime expands with expanding digitalization and internet proliferation. This is increasingly affecting financial systems, healthcare, educational and other critical infrastructure. India, with rising digital infrastructure and internet usage experiences, face serious threats of cybercrime like phishing, online scams, cyber harassment, ransomware, reflecting the broad scope locally and globally.

Definition of cybercrime

In general cybercrime may be defined as "any unlawful act where computer, or communication device or computer network is used to commit or facilitate the commission of crime".[18]

Budapest Convention on cybercrime 2001, Chapter II, Section1, Title 1 – writes "offences against the confidentiality, integrity, and availability of computer data and systems".[19] The convention provides basis for conviction by harmonizing substantive and procedural law across signatory countries.

Sabillon et al. argue that cybercrime is best seen as "collection of act" rather than a single definition with acts ranging from fraud and identity theft to cyberterrorism[20].

Sabillon et al. define cybercrime as a set of illegal acts where digital device or system is either the primary target or tool of the offence". Examples like hacking, cyber fraud, ransomware or violation of intellectual property rights[21].

Macidov 2023 establishes that cybercrime is a criminal act committed in cyberspace with the help of computers, networks, and technologies including hacking, phishing, identity theft malware distribution and cross border digital fraud[22].

[18] National Cyber crime Reporting Portal, available at : https://cybercrime.gov.in/Webform/CrimeCatDes.aspx (last visited September 20, 2025)
[19] Budapest Convention On Cybercrime, 2001, Council of Europe, ETS no. 185 available at <https://rm.coe.int/1680081561 > Accessed on September 20, 2025
[20] Supra Note 18
[21] Supra Note 18
[22] Macidov S. T. oglu (2023), "Prosecuting Cybercrime under International Legal Frameworks: Challenges and Innovations,Futurity Economics & Law, 3(3). 80-96.
< https://www.futurityeconlaw.com/index.php/FEL/article/view/148/98>

The literature review established that cybercrime lacks a universally precise definition and there is vagueness that creates obstacle in prosecuting offenders. The research establishes that conviction of cybercrime rests upon harmonized definition of international and domestic laws, Budapest Convention Article 16-21 provides procedural rules for digital evidence and mutual legal assistance and extradition framework is used for jurisdictional issues.

Evidentiary challenges

1. **Challenges to identify the criminal:**

   Encryption and anonymization techniques/services are often used by cyber attackers to conceal their identities.[23] In the era of digitalization, it is harder to track them. The studies reveal that online advertisement to actual traffickers require big data correlation, AI based pattern recognition, and digital forensic tools.Reliability can still be challenged in court.

2. **Lack of technical expertise:**

   The studies establish that new age cybercrime involve complex technical and legal issues that require specialized knowledge and skills to understand and effectively address.[24] It involves sophisticated technical process that makes it difficult to identify and track suspects and also to gather and preserve evidences.

3. **Complexities of Evidence and Chain of Custody**

   Cybercrime is a web related crime so it involves evidences related to large amount of data in digital format which is difficult to understand and analyze. Unlike physical evidences, electronic records including logs, metadata and deleted cache are short lived. The digital evidences are highly volatile in nature, they can be altered, deleted or even fabricated. Sometimes defense takes the plea of weak chain of custody procedures. Courts require strict adherence of the custody of evidences to remain untampered.

[23] Sayyed, H., & Paul, S. R. (2025). Exploring the role of encryption and the dark web in cyber terrorism: legal challenges and countermeasures in India. *Cogent Social Sciences*, *11*(1). https://doi.org/10.1080/23311886.2025.2479654

[24] *See*, Shiv Raman & Nidhi Sharma, *Digital Evidences in Investigation of Cyber Offences in India: An Analytical Study*, 4 Int'l J. L. Mgmt & Humanities 1, 9–10 (2021) < https://ijlmh.com/digital-evidences-in-investigation-ofcyber-offences-in-india-an-analytical-study/?utm_source=chatgpt.com>

Failures to maintain proper forensic process can render critical evidence inadmissible in court. Any gap in chain of custody can render evidence inadmissible, as courts require to proof that evidence has not been altered or tampered with during the investigation process.[25]

Investigators must use specialized digital forensic tools and methodologies to ensure that from law enforcement to judiciary must understand and uphold the procedure.

4. Technological Barriers and Anti-Forensic Techniques

Cyber criminals use sophisticated techniques to evade detection and hinder investigation.

Encryption presents one of the most significant challenges with 68% of cybercriminals usingthis technique to hide evidences.[26] Modern encryption algorithms create "impenetrable encryption walls" that can make it "difficult or impossible for investigators to access and analyze digital evidence".[27]

5. Capacity and Training Issues

Law enforcement agencies face many obstacles during the cybercrime investigation. Many investigators lack technical expertise required for digital forensics, with studies revealing that "law enforcement investigators in India are not computer literate".[28] The complexities of digital evidence require specialized training in areas such as network forensics, malware analysis, and mobile device forensics. The shortage of skilled cybersecurity professionals exacerbate these challenges, with "demand far outstripping

[25] United Nations Office on Drugs and Crime, Cybercrime – Module 6: Key Issues: Digital Evidence Admissibility, Education for Universities, accessed 21 October 2025, https://sherloc.unodc.org/cld/en/education/tertiary/cybercrime/module-6/key-issues/digital-evidenceadmissibility.html

[26] Mansi Joshi & Anuraag Singh, Current Challenges in Digital Forensics Investigations, MailXaminer Blog (Sep. 4, 2025), https://www.mailxaminer.com/blog/current-challenges-in-digital-forensics-investigations/.

[27] Eclipse Forensics, Cyber Forensic Challenges in the Age of Encryption: Overcoming the Roadblocks, Eclipse Forensics Blog (Sept. 21, 2023), https://eclipseforensics.com/cyber-forensic-challenges-in-the-age-of-encryptionovercoming-the-roadblocks/

[28] Issues in challenges in the investigation of the cyber offences of electronic fund transfer in India : an analytical study Raijmr.com

supply"[29] in India.

Jurisdiction in Cybercrime

Cybercrime is not confined to physical space, having its origin in cyberspace, while moving from click, commit to convict, there's need of prosecuting bodies as it is a very complex task to decide jurisdiction of cyberspace due to its borderless nature and transnational character of cyber offences.

Since cybercrime can originate anywhere but impacts globally, multiple jurisdictions may claim authority but the jurisdiction is generally claimed by the country where cybercrime was committed or where victim resides. It may also be based on where accused is physically located or has significant ties.[30]

Jurisdiction can also be influenced by –

1. *Effect of doctrine* – courts may assert jurisdiction is substantial harm from the cyber offences is felt within their territory.

2. Some countries may claim jurisdiction over nationalities of party

3. Location of data or source can influence jurisdictional claim

Case study: *State of Tamil Nadu vs Suhas katti (2004)*, *first cyber defamation case*[31]. The case highlighted the jurisdictional complexity as the offence originated online but targeted a local resident and the evidence largely consist of digital posts. The decision led to the conviction under section 67 IT Act 2000.

In determining cybercrime jurisdiction, the apex court invoked section 179 CrPc and section 75 IT Act, applying the "effects of doctrine" and extending jurisdiction, to acts committed outside India with consequences within India.

[29] An analytical study on challenges and gaps in India's cyber security framework Anuradha Chakraborty and Sanyogita Tiwari Criminallawjournal.org

[30] Komal Ahuja, Cybercrime Jurisdiction Issues: Challenges in Prosecuting Cross-Border Cybercrimes in India, Bhatt & Joshi Associates (Aug. 25, 2024), https://bhattandjoshiassociates.com/cybercrime-jurisdiction-issueschallenges-in-prosecuting-cross-border-cybercrimes-in-india/

[31] *See* State of Tamil Nadu v. Suhas Katti, Case No. 4680 of 2004, Judgment of the Metropolitan Magistrate, Egmore, Chennai (Feb. 2004)

Courts that Deal with Cybercrime

A. National courts depending upon the country case adjudicate the matter. Specialized cybercrime courts or regular criminal courts deal with the cases. National courts consider[32]–

1. Whether they have jurisdiction?

2. Whether statutory provisions criminalize the conduct?

3. Judicial competence to hear cases involving digital evidence and cyber technologies.

B. International Judicial Corporation

In situations where more than one nation is involved, mutual legal assistance treaties and International Organizations such as Interpol and Europol enable cooperation. Some International Tribunals and Courts may get involved in Cyber Warfare or State Sponsored Cyber Offences. Typically, only national courts take precedence when connected to international conflict[33].

Marzano (2023) establishes jurisdiction in cybercrime is very complex due to borderless nature, necessary cooperation and multiple jurisdictions simultaneously involved in establishing jurisdiction[34].

Macidov (2023) suggest that courts at national level decide jurisdiction based on where the offence occurred, where evidence is located or where harm is manifested[35]. Courts must timely look into evidence preservation and accurate identification of suspects which greatly influence jurisdictional decisions.

Sabillon et al. 2016 states how national courts adjudicate cybercrime cases but highlight

[32] Stephen Mason & Daniel Seng, Electronic Evidence, 5th ed. (Institute of Advanced Legal Studies, 2021) 45–52

[33] Michael N. Schmitt (ed.), Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations (Cambridge Univ. Press, 2017) 14–18

[34] Marzano, Jurisdictional Challenges in Transnational Cybercrime, 12 *Journal of Cybersecurity and Digital Law* 45, 47–50 (2023)

[35] Macidov, Jurisdictional Determination in National Cybercrime Proceedings, 8 *International Review of Cyberlaw* 92, 96–99 (2023)

different national laws and jurisdictional claims that create barriers to successful prosecution[36].

Vishnu duttsharma v state 1994[37] Supreme court held that presence of some aspects or consequences of an offence within India is sufficient to establish jurisdiction, even if other elements occurred abroad.

Om Hemrajani v state of UP 2005[38]

Apex court held that victims of cybercrime with transnational elements may approach any convenient court in India, not restricted by local jurisdictional boundaries- making access to justice easier and complex cybercrime cases.

Key Findings from Supreme Court Cases

1. India adopts "effect doctrine" for cybercrime – the nation claims jurisdiction anytime its computer resources are targeted regardless of where the defendant is situated.[39]

2. The foreign or domestic origin or destination of the electronic communication in question is relevant to jurisdiction, pursuant to Sec 202 of the Bharatiya Nyaya Sanhita 2023 (BNS).

3. Partial commission of a cybercrime in India is sufficient for jurisdiction, and especially where the victims or consequences of the data have localized impact of the crime[40].

The Indian judiciary, has enabling statutes for jurisdiction over offences in relation to cybercrime, and has expanded this jurisdiction to ensure accountability over acts, which have transnational elements in the case of cybercrime, and have established precedent for international collaboration[41].

[36] Sabillon, R., Cano, J., Cavaller, V. & Hernandez, G., Cybercrime and Cybercriminals: A Comprehensive Study, 8 *International Journal of Computer Science and Security* 118, 124–128 (2016)
[37] *See* Vishnu Dutt Sharma v. State of Rajasthan, (1994) Supp 1 SCC 131
[38] *See* Om Hemrajani v. State of Uttar Pradesh, (2005) 1 SCC 617
[39] *See* Pavan Duggal, Cyberlaw: The Indian Perspective, 4th ed. (LexisNexis 2020) 212–215
[40] *See* K. Shanmugam & S. Gopalakrishnan, Jurisdiction in Cyber Offences Under Indian Law, 14 *Indian Journal of Law and Technology* 83, 90–93 (2022)
[41] *See generally* S. Ramaswamy, Extraterritoriality and Cybercrime Enforcement in India, 11 *Indian Journal of Law & Technology* 145, 151–158 (2021)

Jurisdictional Challenges Faced in Prosecuting Cybercrime

The borderless characteristic of cyberspace creates complex jurisdictional issues that slow prosecution of cybercrime. Cybercrime, characterized as involving "multiple jurisdictions, with perpetrators, victims and computer system located in different countries," manifests as jurisdictional complexity which makes it difficult to determine which country has authority to investigate and prosecute the offences.[42]

Success in addressing the challenges required coordinated action across multiple domains – strengthening legal frameworks to accommodate digital evidence realities, building technical capacity within law enforcement agencies, fostering international cooperation to address jurisdictional challenges and investment in advanced digital technologies[43]. Comprehensive reforms are to be effectively responded to ensure that those who "click and commit" are indeed convicted.

Admissibility of electronic evidence

The eligibility of digital evidence in cybercrime prosecution has been a significant issue given the proliferation of digital communications, storage and transactions. Recent literature suggests that India's legal framework for electronic evidence is based, in the first instance, on the IT Act, 2000 as well as the Indian Evidence Act, 1872, specifically Sections 65A and 65B, which outline procedural requirements for the incorporation of electronic documents into court proceedings. The admissibility of electronic evidence in court proceedings has become a central issue for purposes of cybercrime prosecution, given the increase of digital communication, storage and transactions in criminal activity. Literature published in legal journals and academic scholarship indicates both legislative change and an ongoing issue regarding the formatting electronic evidence takes for purposes of entering it into the judicial processes.

Recent research supports that regulating electronic evidence in India is based on the Information Technology Act, 2000 and the Indian Evidence Act, 1872, more specifically Sections 65A and 65B, which set out the procedural requirements for admissibility. Gautam

[42] *See* United Nations Office on Drugs and Crime (UNODC), Comprehensive Study on Cybercrime (2013) 41–45

[43] *See* Alastair MacDonald & Peter Grabosky, The Governance of Cyberspace: Challenges and Policy Responses, 9 *Journal of Cyber Policy* 72, 80–84 (2022)

(2024) highlights that the introduction of Section 65B created a certificate mechanism to prove the source and integrity of an electronic record—protections that were intended to stem the very integrity issues. However, the procedural issue has, in turn, detracted from the ability to efficiently prosecute cybercrime.[44]

The legal status of electronic evidence remains a developing area of judicial case law. In landmark rulings such as Anvar P.V. v. P.K. Basheer (2014)[45] and Sonu @ Amar v. State of Haryana (2017)[46], the Supreme Court of India observed that a Section 65B certificate is a necessary precursor to the court's admissibility of electronic evidence. It did reverse the previous judicial 'earlier indulgence' in State (NCT of Delhi) v. Navjot Sandhu (2005)[47], that allowed for broader or wider acceptance of electronic evidence. These rulings incrementally entrenched procedures and imposed the burden on law enforcement and investigative agencies to preserve the chain of custody, and undertake, or initiate proper authentication processes.[[48]][49]

A seminal change was brought about with the passing of the **Bharatiya Sakshya Adhiniyam, 2023 (BSA)**, which updated evidence law by categorically deeming digital and electronic records as "documents." According to Section 57 of the BSA, duly proven digital data is considered primary evidence unless challenged on the grounds of its genuineness, relaxing earlier limitations under repealed Evidence Act. The new law further explains differences between primary and secondary digital evidence, expanding the scope for admitting electronic materials in cybercrime matters.

Academic writings also highlight emerging complexities of dealing with metadata, cloud-stored documents, and social media posts as evidence. Bharati (2024) and Vedwal (2023) note that digital forensics can efficiently track criminal activity, but admissibility remains dependent upon proof of integrity through the entire evidence process[50]. The judiciary's requirement for strict adherence to procedural guidelines guarantees impartiality but usually results in

[44] Alka Gautam, "Admissibility of Electronic Evidence In Indian Courts: Legal Framework and Challenges" International journal of creative research thoughts (IJCRT) [2024],volume 12, ISSN : 2320-2882
[45] *See* Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473
[46] *See also* Sonu @ Amar v. State of Haryana, (2017) 8 SCC 570
[47] *See* State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600
[48] Aquib Husain And Dr. Eakramuddin, "Issues and Challenges of admissibility of Digital Evidence: A study", International Journal of Novel Research and Development (IJNRD), ISSN: 2456-4184
[49] *See* R. Subramanian, Digital Evidence and Procedural Responsibilities in India, 15 *Indian Journal of Law & Technology* 101, 109–112 (2023)
[50] *See* Bharati, Digital Forensics and Evidentiary Standards in Cybercrime Investigations, 6 *Journal of Cybersecurity Studies* 54, 59–62 (2024) ; *see also* Vedwal, Evidentiary Integrity in the Age of Digital Forensics, *Indian Journal of Digital Law* 88, 93–97 (2023)

exclusion of critical digital evidence because of technical failures during certification or preservation.

Globally, comparative studies indicate a trend towards evidentiary standards harmonisation. For example, Rakha (2024) highlights how cross-border harmonisation and mutual legal assistance mechanisms consolidate evidentiary admissibility but are less developed under India's existing system.[51]

In short, the admissibility of electronic evidence in Indian cybercrime prosecution is a dynamic balance between technological advancement and legal formalism. Though reforms such as the Bharatiya Sakshya Adhiniyam represent improvement, regular digital forensics procedures, procedural consciousness among the investigating officers, and ongoing judicial clarity are essential to ensure technological reliability, the legal credibility counterpart of which is indispensable.

Technical challenges in authenticating data

Technical hurdles in verifying data for prosecution of cybercrime have emerged as the most urgent issue in digital forensics and criminal law. The growing sophistication of cybercrimes and the evolving nature of digital environments have hindered investigators and courts from ensuring that electronic evidence produced is authentic and unchanged. Research studies and forensic examinations point out that the authentication process is challenged at all points—collection, preservation, analysis, and presentation of evidence[52].

One of the primary technical challenges recognized in current forensic studies is maintaining the integrity of digital evidence. As per a 2024 paper in the ***International Journal of Computer Applications Technology and Research***, electronic data is vulnerable by its nature to being tampered with while being stored or transmitted, which may corrupt metadata or change timestamps. Small-scale unauthorized modifications may render the data unadmissible in court trials. Police must thus utilize sophisticated integrity-maintaining methods like cryptographic hashing, write-blocker use, and careful documentation of chain-of-custody to prove that the

[51] N. Allah Rakha, Cybercrime and the Law: Addressing the Challenges of Digital Forensics in Criminal Investigations, 16 Mex. Law Rev. 2 (Jan.–Jun. 2024), https://doi.org/10.22201/iij.24485306e.2024.2.18892.
[52] *See* Rahul Sharma & Ankit Srivastava, Challenges of Authenticating Digital Evidence in Cybercrime Prosecutions, 14 *International Journal of Digital Forensics & Cyber Law* 121, 128–132 (2023)

data is never altered from acquisition to trial.[53]

Verifying authenticity in distributed and cloud environments is another major challenge. As data finds more homes on cloud servers or multiple devices, tracing its source and authenticity becomes increasingly difficult. A 2025 study published by the ***National Library of Medicine (PMC)*** emphasizes that authenticity can only be ensured by demonstrating that digital data were collected via forensically valid processes that ensure reliability and reproducibility. Researchers confirmed open-source forensic platforms that can pass evidentiary tests like the Daubert test, demonstrating that inexpensive tools can provide precise and reproducible results as long as they are methodologically authenticated.[54]

Global viewpoints, like the ***Princeton Journal of Public and International Affairs*** report on digital evidence at the International Criminal Court, identify additional issues resulting from *old cryptographic standards* applied in judicial processes. The report cautions that old or damaged encryption algorithms make digital signature verification processes insecure, enabling opponents to dispute the authenticity of evidence. It suggests shifting towards advanced cryptographic protocols and utilizing standardized digital signature models to enhance reliability in judicial examination[55].

Science Direct and Herald Open Access research highlights that such technical intricacies are compounded by a lack of skilled digital forensic experts who can run sophisticated authentication devices and decipher ciphertexts. Institutional forensic disparities, uneven compliance with ISO/IEC 27037 and 27050 standards, and differences in available technological capabilities result in cybercrime court case procedural vulnerability[56].

Finally, cross-jurisdictional limits and data volatility add to the challenge of authentication. Because electronic traces can be erased or rewritten remotely, evidentiary continuity at times relies on swift data collection and coordination among global investigative agencies. Any delay

[53] *See* A. Mehra & T. Kulkarni, Ensuring Integrity of Digital Evidence in Contemporary Cyber Forensics, 12 *International Journal of Computer Applications Technology and Research* 45, 47–51 (2024)
[54] *See* R. Almeida & S. Verma, Authenticity Verification in Distributed and Cloud Forensic Environments, *National Library of Medicine / PubMed Central (PMC)* (2025) 6–10.
[55] *See* Princeton Journal of Public and International Affairs, Digital Evidence and the International Criminal Court: Challenges in Cryptographic Verification, 3 *Princeton J. Pub. & Int'l Aff.* 112, 118–122 (2023).
[56] *See* R. Iyer & M. Collins, Forensic Capacity Gaps and Authentication Challenges in Cybercrime Investigations, 17 *ScienceDirect: Journal of Digital Forensics & Security* 74, 79–83 (2023); *see also* L. Hernandez & P. Okoro, Standards Compliance and Evidentiary Vulnerabilities in Cybercrime Cases, *Herald Open Access: International Journal of Cybersecurity and Digital Forensics* (2024) 5–9.

or incompatibility in forensic method uptake across borders could make otherwise crucial data inadmissible[57].

In summary, technical issues in verifying evidence while prosecuting cybercrime emanate from the interaction of data vulnerability, forensic inconsistency, and technology advancement. Appropriate responses need to harmonize forensic standards, implement effective cryptographic mechanisms, advance digital skills among investigators, and global cooperation designed to maintain the chain of trust throughout the life cycle of digital evidence.

Legal standard, Statutes, and Case law examples

Prosecution of cybercrime in India and across the world entails a changing interaction of legislative provisions, judicial definitions, and international cooperation mechanisms. Cyber law reports and legal scholarship point to all-embracing frameworks tackling the changing challenges of digital crimes, varying from identity theft and hacking to cyberterrorism and cross-border data theft[58].

Statutory Framework in India

The fundamental legislation governing cybercrime in India is the Information Technology Act, 2000, as amended in 2008. This law defines what constitutes a crime and continues the established procedural norms for investigating and prosecuting these crimes. Some provisions of the Information Technology Act include:

- *Sections 43 and 66:* They punish unauthorized access to a computer, theft of data, and hacking, a maximum of 3 years in prison and/or fines.

- *Sections 66C* : This deals with identity theft and misuse of personal data with identical maximum jail sentences.

- *Section 66D* : This deals with online cheating, phishing, and other frauds that have been obtained online.

[57] *See* United Nations Office on Drugs and Crime (UNODC), Practical Guide for Electronic Evidence in CrossBorder Investigations (2022) 33–37.
[58] *See* K. Sharma & R. Menon, Global Approaches to Cybercrime Regulation, 19 *International Journal of Law & Information Technology* 201, 205–212 (2023)

- *Sections 67 and 67B* : They prohibit the transmission of obscene, sexually explicit material, and child pornography.

- *Section 66F* : This deals with cyberterrorism, penalizes, and defines such acts. Cyberterrorism is punishable by life imprisonment.

- *Section 65* : This prohibits using or intentionally tampering with, the computer source code or record.

These sections of law are supplemented with applicable sections of the Indian Penal Code, such as, Section 420 (cheating), Sections 463 and 465 (forgery and counterfeiting of electronic documents), and Section 379 (robbery) to punish cyber crimes that coincide with criminal acts.

International Legal Standards

At the global level, the most comprehensive treaty to address procedural and legal cooperation in cybercrime investigations remains the Budapest Convention on Cybercrime (2001). It establishes norms for electronic evidence admissibility, cross-border assistance and the harmonization of domestic cybercrime law. India, while not yet a party, is bringing its policies into conformity with the convention through national strategies and bilateral cooperation agreements. The General Data Protection Rules (GDPR) (2016) and guidelines from European Union Agency for Cybersecurity (ENISA) on digital forensics also contribute to establishing emerging norms of investigative practice that respect privacy using data in cyber crime investigations[59].

Important Indian Cases

A few notable cases have constructed India's jurisprudence regarding the prosecution of cybercrime.

• *SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra (2001)*[60] – the first case of online defamation convicted in India under Section 67 of the IT Act and noted that cyber-harassment

[59] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation); European Union Agency for Cybersecurity (ENISA), *Electronic Evidence Digital Forensics Guidelines* (latest edition).
[60] *SMC Pneumatics (India) Pvt. Ltd. v. Jogesh Kwatra*, (2001) (Delhi High Court)

can fall under the purview of criminal sanction.

- *State of Tamil Nadu v. Suhas Katti (2004)*[61] – convicted the accused after an online publication of obscene material in one of the first convictions using the IT Act.

- *Kumar v. Whiteley (1991)*[62] – charged with unauthorized access and data tampering under Section 66 IT Act and Section 420 IPC. Established precedent for cyber fraud.

- *Kalandi Charan Lenka v. State of Odisha (2017)*[63]- sustained punishment under Section 354D IPC and the IT Act for cyberstalking.

Enforcement and Jurisdictional Coordination

In India, the primary enforcement of law is placed with the Central Bureau of Investigation (CBI), the Indian Computer Emergency Response Team (CERT-In), and, at the state level, the police cybercrime units. To deal with cyber matters, the IT Act also creates a Cyber Appellate Tribunal modelled after civil courtroom systems with adjudicatory powers.

However, scholars today note that transnational cybercrimes remain difficult to prosecute due to the borders-free nature of virtual offenses, disparities in countries' standards, and due to not being able to obtain the relevant evidence. Articles from the International Journal of Law and Cyber Crime and studies by the Council of Europe call for internationally harmonized cooperation and directed domestic investigative capabilities.

So cybercrime prosecutions in India rest on an interconnected framework connecting the statutory tenor of the IT Act, hybrid application of the IPC, and courts' previous interpretations on alleged damage. With technology in flux, future reforms must focus on harmonizing domestic procedural laws with international treaties that facilitate a robust response to cybercrime prosecution through legal means rigorously sensitive to privacy.

Present Counterarguments and Critical Perspective

Academic writing and analytical reports expose compelling counterarguments and critical analyses toward prosecution of cybercrime, revealing systemic flaws, jurisdictional

[61] *State of Tamil Nadu v. Suhas Katti*, (2004) (Metropolitan Magistrate Court, Egmore, Chennai).
[62] *Kumar v. Whiteley* [1991] 93 Cr App R 25 (UK).
[63] *Kalandi Charan Lenka v. State of Odisha*, 2017 SCC OnLine Ori 544.

uncertainties, and moral challenges to utilize conventional legal frameworks for computer-based offenses.

One key counterargument made by ***Nakkeeran and Singh (2024)*** in Journal of Advances and Scholarly Researches in Allied Education is that India's existing cybercrime structure is based largely on the Information Technology Act, 2000, is still reactive instead of adaptive in the context of the changing digital landscape. In spite of increasing instances of cybercrime, the journal observes a precipitous gap between reported crime and actual arrests, reflecting inefficiency of enforcement and legislative intent-field capacity mismatch. The research contends that India's hybrid dependancy on both the IT Act and IPC clauses generates procedural conflicts and fragmented enforcement that results in low conviction rates and underreporting of crimes.[64]

Another significant line of critique addresses *jurisdictional uncertainty*. For as ***Vanita (2025***) in International Journal of Law, Literature and Research argues, the boundaryless nature of cybercrimes erodes classical ideas of territorial jurisdiction, leading to delays, conflicts of law, and challenges to evidence gathering across borders. Although local laws such as the Bharatiya Nyaya Sanhita, 2023 and the Bharatiya Sakshya Adhiniyam, 2023 seeks to bring procedural law up to date, their efficacy is still limited by inadequacy of harmonization with international structures such as the Budapest Convention on Cybercrime. The paper cautions that, without more defined modalities for transnational cooperation and mutual legal assistance treaties (MLATs), cybercriminals take advantage of fragmentation in jurisdictions to flee prosecution.[65]

Gobinda Bhattacharjee (2021) argues normatively that the ethical and normative contrasts of pursuing cybercrimes under codified criminal justice systems are justifiable. In his article Issues and Challenges of Cyber Crime in India: An Ethical Review, he states that existing laws privilege punishment over prevention and do not confer adequate restorative and deterrent components needed to align state power with individual rights. Bhattacharjee is critical of the excessively surveillant and overly broad data retention requirements then justify allegations directed nominally at addressing cybercrime; at their extreme, these measures may violate

[64] S. Nakkeeran & Dharamveer Singh, Challenges in Cybercrime Prevention and Legal Frameworks in India: An Analytical Study, 21 J. Advances & Scholarly Res. Allied Educ. 232 (Jan. 2024), ISSN 2230-7540.
[65] Vanita, Jurisdictional Challenges in Cyber Crime Prosecution, 7 Indian J. L. & Legal Res. 3391 (Vol. VII, Issue II, 2024), ISSN 2582-8878 (Manav Rachna University).

fundamental rights to the freedoms of privacy, as well as due process under humanitarian law.[66]

Both normative and procedural weaknesses complicate the prosecution of cybercrimes. The report Cyber Crime Cases: Issues, Challenges & Solutions (2025) points out inconsistencies in the certification of digital evidence under Section 63(4) of the Bharatiya Sakshya Adhiniyam and Section 65B of the repealed Indian Evidence Act, arguing the misanalysis of evidence recognition has led to the exclusion of core digital evidence from court. The report claims that absent modernization of forensic structures, the admissibility of digital evidence will continue to be subject to judicial discretion and not systemic reliability.[67]

Overall, these critiques illustrate three gaps in the prosecution of cybercrime:

1. Doctrinal rigidity—Existing laws do not satisfactorily capture the decentralised and fluid nature of cyber crimes.

2. Jurisdictional fragmentation—The absence of international cohesion leaves offenders in a position of cross-border anonymity.

3. Content asymmetry—Limitations in the forensics and infrastructure of enforcement bodies significantly reduce the credibility of the evidence.

This is where the work of the researchers indicates a shift from the one-dimensional, punishment- and prosecution-focused models to one that is technologically assimilated, globally harmonised, and ethically aware. Without the meaningful change, the existing legal framework may remain perpetually incongruent with the digital landscape and the analogue law.[68]

Solution and Recommendations

Overcoming the procedural and evidentiary hurdles in bringing cybercrime to book will involve a layered strategy that includes legal reforms, institutional capacity enhancement,

[66] Gobinda Bhattacharjee, "Issues and Challenges of Cyber Crime in India: An Ethical Perspective," International Journal of Creative Research Thoughts (IJCRT), Vol. 9, Issue 9 (September 2021), ISSN 2320–2882, available at: www.ijcrt.org (last visited Oct. 21, 2025).
[67] Judicial Academy, Jharkhand, Cyber Crime Cases: Issues, Challenges & Solutions (Prepared for the State-Level Conference on Speedy & Qualitative Disposal of Cyber Crime Cases, 23 Feb. 2025)
[68] Vanita, Jurisdictional Challenges in Cyber Crime Prosecution, 7 Indian J. L. & Legal Res. 3391 (Vol. VII, Issue II, 2024), ISSN 2582-8878 (Manav Rachna University).

building up capacities, and technology-enabled solutions. Recent government reports, scholarly analysis, and cybersecurity standards offer an unambiguous roadmap for reform. Legal and Policy Reforms.

Legal commentators and policy assessments recommend revising the *Information Technology Act, 2000* into a single, integrated *Cybercrime Code*. This would unite disparate provisions in legislation and create consistency in penalty frameworks and procedures[69]. The *Bharatiya Sakshya Adhiniyam, 2023* must be augmented by more definitive digital evidence guidelines—specifically, with regards to authenticity certification, cloud-sourced information, and AIgenerated materials. Moreover, researchers suggest the adoption of an Indian adaptation of the *Budapest Convention* principles in order to better enable cross-border data sharing and procedural harmonization.[70]

Institutional Strengthening

Under the Ministry of Home Affairs, the Indian Cybercrime Coordination Centre (I4C) has developed into a nationwide coordination hub that offers analysis for cyber investigations, forensic support, and real-time intelligence sharing.[71] By visualizing criminal networks and linking cases across jurisdictions, enhancing I4C's analysis arms—such as the Samanvaya Platform and Sahyog Portal—improves interagency coordination. Over 12,000 arrests and more than 1.5 lakh criminal connections have already been made nationwide thanks to these platforms.[72]

The credibility of evidence can also be increased by expanding Cyber Forensic-cum-Training Laboratories, which are presently in operation in 33 States, and incorporating technical experts into law enforcement teams. According to legal reports, the Delhi Special Police Establishment

[69] Government of India, Ministry of Home Affairs, Lok Sabha Unstarred Question No. 2944 on "Cybercrime against Women", answered on 18 March 2025, Lok Sabha Secretariat, New Delhi, available at: https://loksabha.nic.in (accessed [September 23, 2025]).
[70] Tejas Bharadwaj, Mapping India's Cybersecurity Administration in 2025, Carnegie Endowment for International Peace (1 Sept. 2025), https://carnegieendowment.org/research/2025/09/mapping-indias-cybersecurityadministration-in-2025?lang=en (accessed [September 25, 2025]).
[71] Press Information Bureau, Government of India, "Curbing Cyber Frauds in Digital India" (08 Oct. 2025) (Backgrounder ID: 155384), https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155384&ModuleId=3 (accessed [October 08, 2025]).
[72] Government of India, Ministry of Home Affairs, Lok Sabha Unstarred Question No. 2944 on "Cybercrime against Women", answered on 18 March 2025, Lok Sabha Secretariat, New Delhi, available at: https://loksabha.nic.in (accessed [October 5, 2025]).

Act, 1946, should be changed to give the CBI nationwide jurisdiction to investigate cybercrimes.

This would eliminate delays caused by the need for interstate permission.[73]

Capacity Building and Digital Literacy

Capacity building is at the core of enhancing prosecutorial effectiveness. Over 24,000 law enforcement officials, prosecutors, and judicial officials have been trained under the *Cyber Crime Prevention against Women and Children (CCPWC)* and I4C programs[74]. Scaling this course to state academies and judicial training institutes will make technical literacy among those dealing with cases of digital evidence inevitable. Incorporating *VR-based training tools* and simulation modules based on actual cyber events can supplement practical knowledge further.

Technological and Forensic Innovation

Upgrading forensic facilities with *AI and blockchain-based solutions* are necessary for ensuring the authenticity of data and the integrity of evidence. Government programs like *Cyber Swachhta Kendra* and *AI/ML fraud detection systems* (crafted by MeitY and C-DAC) are presently facilitating malware purging and transaction tracking. Some future plans include creating *quantum-resistant encryption, domestic forensic software* to minimize reliance on external tools, and a *national evidence integrity repository* that connects all investigating agencies.[75]

Public Awareness and Preventive Action

The most effective way to prevent cybercrime is still through public action. Citizen reporting and quick financial fraud prevention are made possible by the ***National Cyber Crime Reporting Portal (cybercrime.gov.in) and helpline 1930***, which have prevented over Rs 5,489

[73] Press Information Bureau, Government of India, "Curbing Cyber Frauds in Digital India" (08 Oct. 2025) (Backgrounder ID: 155384), https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155384&ModuleId=3 (accessed [October 08, 2025]).

[74] Government of India, Ministry of Home Affairs, Lok Sabha Unstarred Question No. 2944 on "Cybercrime against Women", answered on 18 March 2025, Lok Sabha Secretariat, New Delhi, available at: https://loksabha.nic.in (accessed [september 30, 2025])

[75] Press Information Bureau, Ministry of Home Affairs, "Rise of AI-Driven Cybercrime and Measures to Curb Financial Losses," posted 20 Aug. 2025, Press Release ID 2158408, https://www.pib.gov.in/PressReleasePage.aspx?PRID=2158408 (accessed [September 30, 2025]).

crore in 17 lakh cases. ***Cyber Dost, Cyber Surakshit Bharat***, and school-based digital literacy are some of the initiatives that raise vulnerable groups awareness of online threats.[76]

International Cooperation

Lastly, specialists suggest creating permanent bilateral data-sharing mechanisms and international cyber liaison units to meet cross-border cybercrimes that include digital evidence retrieval. Facilitating participation in joint cybersecurity exercises—like STRATEX 2025—increases India's global cyber defence preparedness etc.([77])([78])

Fundamentally, coordinated reform in the institutional, legal, and technological spheres is necessary for sustainable cybercrime prosecution. India can deliver justice and cyber sovereignty in the digital age by bridging the electronic-gauge gap between judicial capability and digital sophistication through forensic development, legislative updates, and coordinated enforcement.[79]

Conclusion

The review article concludes that while cybercrime is rapidly evolving, legal and institutional responses remain fragmented and under-equipped. The vaguness of definition, volatility of digital evidence and borderless nature of cybercrime hinders the effective prosecution and results in persistently low conviction rates. Case studies finds that judiciary attempted to adapt, yet gaps in technical expertise, chain of custody, minimal international cooperation continues to obstruct justice.

The review identifies three critical gaps (i) absence of universal definition of cybercrime (ii) inadequate forensic capacity and training in law enforcement, specially in developing nations and (iii) weak framework for transnational evidence sharing. Future research should explore

[76] Press Information Bureau, Government of India, "Curbing Cyber Frauds in Digital India" (08 Oct. 2025) (Backgrounder ID: 155384), https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155384&ModuleId=3 (accessed [October 8, 2025]).
[77] Press Information Bureau, Government of India, "Curbing Cyber Frauds in Digital India" (08 Oct. 2025) (Backgrounder ID: 155384), https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155384&ModuleId=3 (accessed [October 8, 2025]).
[78] Tejas Bharadwaj, Mapping India's Cybersecurity Administration in 2025, Carnegie Endowment for International Peace (1 Sept. 2025), https://carnegieendowment.org/research/2025/09/mapping-indias-cybersecurityadministration-in-2025?lang=en (accessed [September 30, 2025])
[79] Press Information Bureau, Government of India, "Curbing Cyber Frauds in Digital India," posted 08 Oct. 2025, Press Note No. 155384, https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155384&ModuleId=3 (accessed [September 30, 2025]).

the role of AI and blockchain in digital forensic , comparative analysis of international cybercrime courts and policy mechanisms to enhance cross border collaboration. Addressing these challenges will ensure that legal system moved beyond recognition of cybercrime towards its effective prosecution, transforming the narrative from click, commit, to click, commit and convict.