Page 384 - 401 **DOI:** *https://doi.org/10.63108/IJLMH.12833*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 5

2026

The Rising Threat of Cybercrime in India: Legal Challenges, Enforcement Mechanisms, and Emerging Trends

ESHAN SINGHAL[*] AND PROF. (DR.) SHITI KANTH DUBEY[**]

ABSTRACT

The rapid digitisation of economic, social and governmental activities has transformed the nature of criminality and created new challenges for contemporary criminal justice systems. India, as one of the world's largest digital economies, has experienced a substantial expansion of cybercrime, ranging from identity theft, online cheating and cyberstalking to ransomware, financial fraud, deepfakes and other technology-enabled offences. The National Crime Records Bureau's Crime in India 2024 indicates a significant increase in registered cybercrime cases, demonstrating the growing importance of an effective legal and institutional response. Against this background, this paper examines India's cybercrime regulatory framework through a doctrinal and comparative legal methodology. It analyses the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Nagarik Suraksha Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, and related regulatory mechanisms. Particular attention is given to jurisdiction, electronic evidence, attribution of criminal responsibility, intermediary responsibility, cross-border investigation and emerging technology-enabled offences. The study further compares India's approach with selected international frameworks, particularly the Budapest Convention on Cybercrime and the regulatory approaches adopted by the European Union, the United Kingdom and the United States. The paper argues that India's principal difficulty is not the complete absence of cybercrime legislation but the fragmentation of applicable legal provisions across substantive, procedural and regulatory instruments. It concludes that an effective response requires greater doctrinal coherence, specialised investigative capacity, improved electronic-evidence procedures, strengthened international cooperation and a technologically neutral legal framework capable of addressing emerging forms of cybercrime without unnecessarily restricting legitimate digital activity.

Keywords: *Cybercrime, Information Technology Act, Electronic Evidence, Digital Crime, Cybersecurity*

[*] Author is a Ph.D. Research Scholar at the Faculty of Law, Agra College, Dr. Bhimrao Ambedkar University, Agra, Uttar Pradesh, India.

[**] Author is a Professor at the Faculty of Law, Agra College, Dr. Bhimrao Ambedkar University, Agra, Uttar Pradesh, India.

 [ISSN 2581-5369]

I. INTRODUCTION

Digital technology has fundamentally altered the manner in which individuals communicate, conduct commercial transactions, access public services and participate in social and economic life. The expansion of internet connectivity, smartphones, digital payments, cloud computing, social media and artificial intelligence has generated substantial economic and social benefits.[1] At the same time, these developments have created new opportunities for criminal activity. Contemporary cybercrime is no longer confined to conventional forms of computer hacking. It encompasses a broad spectrum of conduct, including unauthorised access to computer systems, identity theft, online impersonation, financial fraud, cyberstalking, ransomware, unlawful interception, data theft, cyber extortion, sexual exploitation, misinformation-enabled fraud and increasingly sophisticated forms of artificial-intelligence-assisted offending.[2]

The legal significance of this transformation lies in the fact that cyberspace does not conform neatly to traditional concepts of territorial criminal jurisdiction. A single cyber offence may involve a victim located in one country, an offender operating from another, servers situated in a third jurisdiction and digital assets transferred through multiple additional jurisdictions.[3] India presents an especially important case for examining these challenges. The country has experienced rapid digitalisation in banking, commerce, governance and communications. At the same time, cybercrime has emerged as an increasingly significant category of reported criminal activity. The National Crime Records Bureau's Crime in India 2024 report records a substantial rise in registered cybercrime compared with the preceding year.[4] India's principal dedicated cybercrime statute remains the IT Act, 2000.[5] Enacted at a time when electronic commerce and digital transactions were developing rapidly, the legislation provided legal recognition to electronic records and electronic communications while also creating specific offences relating to computer resources and electronic activity. The Act subsequently became a central component of India's cybercrime framework.

---

[1] Mohd Javaid et al., *Digital Economy to Improve the Culture of Industry 4.0: A Study on Features, Implementation and Challenges*, 2 GREEN TECH. AND SUSTAINABILITY 1, 11 (2024).

[2] Neil Catton, *Cybercrime in Today's World – The Digital Battlefield We Can't Ignore*, GLOBAL CONSORTIUM GROUP (Mar. 2025), https://globalconsortiumgroup.com/our-work/news/cybercrime-in-todays-world/.

[3] Gargi Sarkar et al., *Assessing the Anticipated Impact of the United Nations Convention Against Cybercrime in India and Beyond*, 13 J. OF ECO. CRIMINOLOGY 1, 8 (2026).

[4] Vijaita Singh, *Rise in Cybercrime but Overall Crime Rate Dropped in 2024, Says Latest NCRB Report*, THE HINDU (May 7, 2026), https://www.thehindu.com/news/national/rise-in-cybercrime-but-overall-crime-rate-dropped-in-2024-says-latest-ncrb-report/article70948292.ece.

[5] The Information Technology Act, 2000, INDIA CODE (2000).

 [ISSN 2581-5369]

However, India's contemporary cybercrime framework cannot be evaluated solely by reference to the IT Act. The commencement of the BNS, 2023,[6] the BNSS, 2023,[7] and the BSA, 2023[8] on July 1, 2024 has altered the broader criminal-law environment in which cyber offences are investigated and prosecuted. This paper argues that India's principal cybercrime problem is not the complete absence of legislation but the fragmentation of the legal response across substantive criminal law, cyber-specific legislation, criminal procedure, evidence law, intermediary regulation and institutional mechanisms. Although India possesses several important legal instruments, their effectiveness depends upon their interaction. The paper has four principal objectives:

- To examine the evolution and present structure of India's legal framework governing cybercrime.
- To analyse the substantive, procedural and evidentiary challenges involved in the investigation and prosecution of cyber offences.
- To comparatively examine India's approach against selected international cybercrime frameworks.
- To propose legal and institutional reforms for strengthening India's response to contemporary and emerging cybercrime.

II. Conceptualising Cybercrime

The absence of a universally accepted definition of cybercrime creates an initial conceptual difficulty. The term is often used broadly to describe any criminal activity involving computers, networks, digital communications or electronic data.[9] However, a useful analytical distinction can be drawn between cyber-dependent crimes and cyber-enabled crimes. Cyber-dependent crimes are offences that require information and communication technologies for their commission. Unauthorised access to computer systems, malware deployment, distributed denial-of-service attacks and certain forms of ransomware fall within this category.[10] Without the existence of computer systems or networks, such offences could not be committed in their contemporary form. Cyber-enabled crimes, by contrast, are conventional forms of criminal conduct whose scale, reach or method has been transformed by digital technology. Online

[6] The Bharatiya Nyaya Sanhita, 2023, India Code (2023).
[7] The Bharatiya Nagarik Suraksha Sanhita, 2023, India Code (2023).
[8] The Bharatiya Sakshya Adhiniyam, 2023, India Code (2023).
[9] Mark Coeckelbergh, *Artificial Intelligence, Responsibility Attribution, and a Relational Justification of Explainability*, 26 Sci. Eng. Ethics 2051, 2065 (2020), https://doi.org/10.1007/s11948-019-00146-8.
[10] Rosario Girasa, Artificial Intelligence as a Disruptive Technology: Economic Transformation and Government Regulation (Palgrave Macmillan, 2nd edn., 2025).

 [ISSN 2581-5369]

cheating, identity fraud, financial deception, stalking, harassment, extortion and sexual exploitation may occur without computers, but digital platforms enable offenders to conduct these activities rapidly and across geographical boundaries.

India's statutory framework reflects this hybrid character. The IT Act contains specifically technology-oriented offences, while the BNS continues to provide general offences capable of application where digital technologies are merely the means through which criminal conduct is performed. For example, the BNS contains offences whose commission may occur through electronic means without necessarily requiring a separate cybercrime provision. Similarly, the BNSS provides jurisdictional rules for offences involving cheating through electronic communications.[11] It permits such offences to be inquired into or tried in jurisdictions where the electronic communication was sent or received and, in relevant cases, where property was delivered or received. However, the rapid evolution of digital technologies has generated cybercrime forms that expose the limitations of static statutory categories. Some of the new vectors of cybercrime are discussed below.

A. Ransomware

Ransomware involves malicious software that restricts access to systems or data, frequently accompanied by demands for payment. Modern ransomware operations may involve data exfiltration followed by threats to publish stolen information. The criminal conduct may therefore simultaneously involve unauthorised access; data interference; extortion; identity theft; financial offences; and offences involving confidential information.[12] This demonstrates why cybercrime cannot be regulated effectively through a single offence provision.

B. Deepfake-Enabled Fraud

Deepfake technology creates another significant legal challenge. An offender may use synthetic video or audio to impersonate government officials, corporate executives, relatives, financial advisers, public figures or other trusted persons.[13] The resulting harm may include financial fraud, reputational injury, identity theft, sexual exploitation or political manipulation.

Existing provisions concerning cheating, personation, privacy and electronic records may apply depending on the facts. However, the emergence of synthetic media raises the question of whether the law should expressly recognise technologically generated impersonation. A

[11] The Bharatiya Nagarik Suraksha Sanhita, 2023, INDIA CODE (2023), § 202.
[12] Marc Schmitt & Ivan Flechais, *Digital Deception: Generative Artificial Intelligence in Social Engineering and Phishing*, 57 AI REVIEW 1, 10 (2024).
[13] Bart van der Sloot & Yvette Wagensveld, *Deepfakes: Regulatory Challenges for the Synthetic Society*, 46 COMP. LAW & SECURITY REV. 1, 18 (2022), https://doi.org/10.1016/j.clsr.2022.105716.

 [ISSN 2581-5369]

technologically neutral approach is preferable to legislation that attempts to enumerate every new form of synthetic media. The critical legal elements should remain the conduct, intention, harm and method of deception rather than the particular software used.

C. Digital Arrest Scams

A particularly important contemporary form of cyber fraud involves impersonation of law-enforcement officers, regulators or judicial authorities through telephone or video communication. Victims may be falsely informed that they are implicated in a criminal investigation and instructed to transfer money for "verification," "bail," "security" or other fabricated purposes. Such conduct demonstrates the convergence of technology and psychological manipulation. The technical component may be relatively simple, but digital communication dramatically increases the offender's ability to impersonate trusted institutions.

The legal response therefore requires cooperation between cybercrime investigators, financial institutions, telecommunications providers and digital platforms.

D. Cryptocurrency-Enabled Cybercrime

Cryptocurrencies and virtual digital assets can complicate financial investigation because transactions may occur across decentralised networks and pseudonymous addresses.[14] However, pseudonymity should not be equated with complete anonymity. Blockchain analysis can sometimes identify transaction patterns and links between wallets. The principal legal challenge is therefore not simply criminalising cryptocurrency-related conduct but developing the forensic and investigative capacity necessary to trace digital assets and establish the connection between a wallet and an identifiable offender.

III. Evolution of India's Cybercrime Legal Framework

India's dedicated cyber legislation originated in the context of increasing electronic commerce and the growing importance of electronic records. The IT Act, 2000 was enacted with the primary objective of granting legal recognition to electronic transactions and electronic communications while establishing a regulatory structure for digital activity. The Act came into force on October 17, 2000. The original legislative design was consequently broader than criminal law. Cybercrime regulation was only one component of a statute principally concerned with electronic commerce, electronic records and digital signatures. As digital technology evolved, however, cyber offences became increasingly prominent, resulting in amendments and

[14] Nadia Khadam et al., *How to Punish Cyber Criminals: A Study to Investigate the Target and Consequence Based Punishments for Malware Attacks in UK, USA, China, Ethiopia & Pakistan*, 9 HELIYON 1, 22 (2023), https://pmc.ncbi.nlm.nih.gov/articles/PMC10709485/.

the development of additional provisions addressing computer-related offences.[15] The later framework introduced specific offences dealing with computer-related wrongdoing, identity theft, online personation, privacy violations, sexually explicit electronic content and cyber terrorism. The structure of the present IT Act demonstrates this expansion. Chapter XI contains offences, while subsequent provisions address intermediary liability and other regulatory matters.

The constitutional and judicial development of Indian cyber law has also influenced the regulatory environment. A prominent example is the Supreme Court's decision in *Shreya Singhal*, in which section 66A of the IT Act was struck down as unconstitutional.[16] This decision illustrates an important principle in cybercrime legislation: technological regulation cannot be separated from constitutional guarantees of freedom of speech and expression. The development of cyber law therefore reflects a continuing tension between two objectives: first, enabling effective prevention and investigation of digital crime; and second, protecting constitutional rights, privacy, freedom of expression and procedural fairness. This tension has become more significant with the increasing use of government powers relating to interception, monitoring, blocking, data preservation and intermediary compliance.

The next major transformation occurred through India's comprehensive replacement of the principal colonial-era criminal statutes by the BNS, BNSS and BSA. Their relevance to cybercrime lies not merely in the creation of new offences but in the integration of electronic communications and electronic processes into the ordinary criminal justice system. The BNSS, for example, expressly recognises electronic communication in the process of reporting offences and provides that information concerning a cognizable offence may be given electronically, subject to the statutory requirement concerning authentication by the informant.[17] Similarly, it also recognises the importance of electronic devices during investigation and requires the police report to include the sequence of custody where an electronic device is involved.[18] This is particularly significant because the reliability of digital evidence depends not merely on its existence but also on demonstrating how the evidence was collected, preserved and handled. The legislative transition therefore presents an opportunity to move away from viewing cybercrime as a specialised exception to ordinary criminal law.

[15] Hitesh Bhatt, *Industry 4.0 Crime Scene Investigation: A Review and Zero-Trust Digital Forensic Architecture for Evidence Integrity*, 14 FORENSIC SC. INT. REPORTS 1, 18 (2026).
[16] *Shreya Singhal v. Union of India*, AIR 2015 SC 1523.
[17] The Bharatiya Nagarik Suraksha Sanhita, 2023, INDIA CODE (2023), § 173.
[18] The Bharatiya Nagarik Suraksha Sanhita, 2023, INDIA CODE (2023), § 193.

 [ISSN 2581-5369]

Instead, digital technology is increasingly incorporated into the general architecture of criminal investigation and adjudication.

IV. The Information Technology Act, 2000 and Substantive Cybercrime

The IT Act remains the principal specialised legislation governing cyber offences in India. Its importance arises from the fact that several forms of digital wrongdoing require legal provisions in which the technological component is itself an element of the offence.

A. Unauthorised Access and Computer-Related Offences

The IT Act forms an important foundation for addressing unauthorised acts involving computer systems. It provides for liability in specified circumstances involving unauthorised access, downloading, introducing contaminants, damaging computer resources and related conduct,[19] and also criminalises specified acts when performed dishonestly or fraudulently.[20] The structure reflects a distinction between civil liability and criminal culpability. This distinction is doctrinally significant because not every unauthorised digital act should automatically attract criminal punishment. Criminal liability requires the statutory mental element specified by the legislation.

B. Identity Theft

The IT Act, 2000 addresses identity theft and criminalises fraudulent or dishonest use of another person's electronic signature, password or unique identification feature.[21] The provision has become increasingly important in an environment where authentication credentials function as gateways to banking, social media, e-commerce and government services. However, the provision also illustrates a broader limitation of offence-specific cyber legislation. Digital identity today may involve biometric identifiers, device identifiers, behavioural authentication, facial recognition and synthetic identities. The concept of a "unique identification feature" therefore requires interpretation capable of accommodating technological development without violating the principle of legality.

C. Cheating by Personation

The IT Act, 2000 addresses cheating by personation through a computer resource or communication device.[22] The provision is particularly relevant to online financial fraud,

[19] The Information Technology Act, 2000, INDIA CODE (2000), § 43.
[20] The Information Technology Act, 2000, INDIA CODE (2000), § 66.
[21] The Information Technology Act, 2000, INDIA CODE (2000), § 66C.
[22] The Information Technology Act, 2000, INDIA CODE (2000), § 66D.

 [ISSN 2581-5369]

impersonation of officials and fraudulent digital communications. The growth of social engineering has further complicated the distinction between conventional cheating and technologically facilitated personation. A doctrinal challenge arises when an offender uses multiple technological layers, such as spoofed telephone numbers, fake websites, anonymous accounts and cryptocurrency wallets. Although the substantive offence may be relatively straightforward, establishing the identity and *mens rea* of the actual offender becomes considerably more difficult.

D. Violation of Privacy and Cyber Terrorism

The IT Act, 2000 criminalises specified violations of privacy involving private images.[23] The provision has considerable contemporary relevance given the growth of non-consensual dissemination of intimate images, manipulated images and digitally altered representations. Nevertheless, emerging technologies such as generative artificial intelligence[24] and deepfakes expose limitations in legislation drafted before such technologies became widespread. A synthetic image may depict a real individual without necessarily involving an original photograph captured from the person's private space. This raises questions regarding whether existing statutory categories adequately capture the harm. On the other hand, the Act also addresses cyber terrorism. Its existence demonstrates that Indian cybercrime law recognises that digital attacks may extend beyond private financial or personal harm and may affect national security.[25] The challenge, however, lies in distinguishing serious cybercrime from conduct sufficiently grave to constitute cyber terrorism. Overbroad application of national-security provisions may create concerns regarding proportionality and constitutional safeguards.

V. The Post-2024 Criminal-Law Framework and Cybercrime

The BNS, BNSS and BSA should not be regarded as replacements for the IT Act in the field of cybercrime. Instead, they form part of a layered framework. The BNS provides general substantive criminal law. The BNSS governs investigation, arrest, inquiry and trial. The BSA governs evidentiary questions.[26] The IT Act provides specialised provisions addressing technology-specific conduct. This layered structure is potentially advantageous because cybercrime can involve both technology-specific and technology-neutral criminal conduct. However, it also creates a risk of fragmentation. For instance, a fraudulent digital investment

[23] The Information Technology Act, 2000, India Code (2000), § 66E.
[24] Ramanpreet Kaur et al., *Artificial Intelligence for Cybersecurity: Literature Review and Future Research Directions*, 97 Info. Fusion 1, 26 (2023), https://doi.org/10.1016/j.inffus.2023.101804.
[25] The Information Technology Act, 2000, India Code (2000), § 66F.
[26] Antony Nicolas Allott, *General Principles of Criminal Law*, Encyclopaedia Britannica (July 22, 2026), https://www.britannica.com/topic/crime-law/General-principles-of-criminal-law.

scheme may involve: cheating under general criminal law; cheating by personation under the IT Act; identity theft; unauthorised access; manipulation of electronic records; money laundering; and offences under financial-sector legislation. The prosecution must therefore determine which statutory provisions apply to the particular factual circumstances and how they interact.

Nevertheless, technological facilitation of criminal procedure should not be confused with the solution to cybercrime investigation. Digital proceedings may increase efficiency, but they do not resolve questions of authenticity, attribution, chain of custody, cross-border data access or reliability. One of the most significant legal developments affecting cybercrime prosecution is the formal integration of electronic and digital evidence into the evidentiary framework of the BSA, 2023. Its structure expressly addresses electronic or digital records, provides that the admissibility of such a record cannot be denied merely because it is electronic or digital, and gives such records the same legal effect, validity and enforceability as other documents,[27] and it establishes the principal framework for the admissibility of electronic records.[28] It provides circumstances in which computer output may be treated as a document and admitted without production of the original, subject to specified statutory conditions.

A. From Section 65B to the BSA

Before the BSA, electronic evidence was principally governed by section 65B of the Indian Evidence Act, 1872. The Supreme Court's jurisprudence in *Anvar P.V.*[29] established the importance of compliance with section 65B for admitting electronic records. The Supreme Court subsequently clarified the operation of section 65B in *Arjun Panditrao*,[30] reaffirming the importance of the statutory certificate for secondary electronic evidence in circumstances governed by the provision. The BSA replaces the earlier statutory framework but retains a structured approach toward electronic records. The transition is significant for cybercrime law because it demonstrates that electronic evidence is no longer a peripheral evidentiary category. It has become a central component of criminal adjudication.

B. Authenticity and Reliability

Admissibility, however, is not equivalent to reliability. A screenshot of a social-media conversation may demonstrate the apparent existence of communication, but it may not independently establish:

[27] The Bharatiya Sakshya Adhiniyam, 2023, INDIA CODE (2023), § 61.
[28] The Bharatiya Sakshya Adhiniyam, 2023, INDIA CODE (2023), § 63.
[29] *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473.
[30] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

 [ISSN 2581-5369]

- who created the account;
- who controlled the account at the relevant time;
- whether the communication was altered;
- whether the screenshot represents the complete conversation;
- whether metadata has been preserved;
- whether the device itself was compromised; or
- whether another individual had access to the account.

This distinction is especially important in cybercrime because digital evidence can be manipulated with increasing sophistication. Deepfake technology further complicates the problem. Audio, video and images can be synthetically generated or altered in ways that may be difficult to detect through ordinary observation. A future-ready evidentiary framework must therefore distinguish between the formal admissibility of electronic records and the substantive reliability and authenticity of their contents.[31]

C. Chain of Custody

The BNSS complements the BSA by recognising the importance of electronic devices in investigation. Its provisions concerning police reports require the sequence of custody to be addressed where an electronic device is involved. This is an important development because the evidentiary value of a digital device depends substantially upon demonstrating how it was seized, preserved, examined and transferred. A robust chain of custody should ordinarily establish: seizure → identification → preservation → forensic acquisition → examination → storage → transfer → production before court. Any unexplained gap can provide the defence with an opportunity to challenge authenticity or integrity. Accordingly, India's cybercrime framework should move toward nationally standardised digital-forensics protocols, including uniform procedures for imaging devices, generating hash values, documenting forensic examination and maintaining secure evidence repositories.

VI. Institutional Framework for Cybercrime Enforcement in India

The effectiveness of cybercrime legislation ultimately depends upon the institutional capacity available for its implementation. Unlike conventional offences, cybercrime frequently requires investigators to possess specialised knowledge concerning computer networks, digital forensics, electronic communications, cryptocurrency transactions, cloud infrastructure and

[31] Athina Sachoulidou, *AI Systems and Criminal Liability: A Call for Action*, 11 Oslo Law Rev. 1, 9 (2024), https://doi.org/10.18261/olr.11.1.3.

 [ISSN 2581-5369]

data preservation. Consequently, the mere enactment of substantive offences cannot ensure effective cybercrime control unless law-enforcement institutions possess the technical and procedural capacity necessary to investigate such offences. India has progressively developed a multi-layered institutional architecture for addressing cybercrime. At the central level, the Ministry of Home Affairs plays a significant coordinating role through the Indian Cyber Crime Coordination Centre ("I4C").[32] The I4C scheme was approved in 2018 and was subsequently established as an attached office of the Ministry of Home Affairs on July 1, 2024. The I4C structure consists of several specialised components, some of which are discussed below.

A. National Cybercrime Reporting Portal

The National Cybercrime Reporting Portal provides an important mechanism for reporting cybercrime incidents. This centralised reporting can assist in identifying patterns involving the same telephone numbers, bank accounts, cryptocurrency addresses, websites and social-media accounts. This is particularly important in cases of organised cyber fraud. If each complaint remains confined to an individual police jurisdiction, investigators may fail to recognise the common infrastructure connecting apparently unrelated offences. Centralised information can facilitate intelligence-led investigation and identification of organised cybercrime networks. However, reporting infrastructure cannot by itself solve the problem of under-reporting. Victims may refrain from reporting because of embarrassment, complexity of legal procedures or the belief that recovery of lost funds is unlikely. Cybercrime policy must therefore combine accessible reporting mechanisms with effective investigation and victim-support mechanisms.

B. Cybercrime Investigation and Forensic Capacity

Digital evidence is fundamentally different from many forms of conventional evidence. A physical object normally remains relatively stable after seizure, whereas digital evidence can be copied, modified, encrypted, remotely deleted or altered without obvious physical signs. Investigators must therefore preserve not only the content of digital information but also the circumstances in which it was acquired. The institutional challenge is particularly acute in cases involving cloud computing, encrypted communications and distributed infrastructure. The I4C's National Cyber Forensic Laboratory ecosystem and National Cybercrime Training Centre are therefore significant institutional developments. The official I4C framework specifically identifies forensic support, investigation and training among its principal functions. Nevertheless, institutional centralisation should not produce excessive dependence upon a

[32] Khushi, *Indian Cyber Crime Coordination Centre (I4C): Strengthening India's Response to Cyber Fraud*, IMPRI IMPACT AND POLICY RESEARCH INSTITUTE (Aug. 16, 2026), https://www.impriindia.com/centres/center-for-ict-for-development/indian-cyber-crime-coordination-centre-i4c-strengthening-indias-response-to-cyber-fraud/.

 [ISSN 2581-5369]

single national agency. Cybercrime investigation is primarily undertaken by State and local law-enforcement agencies. Consequently, the long-term effectiveness of the framework depends upon the ability to distribute specialised knowledge and forensic capacity throughout the criminal justice system.

VII. Jurisdictional Challenges in Cybercrime

Territorial jurisdiction represents one of the most difficult problems in cybercrime enforcement. Traditional criminal law generally associates jurisdiction with the place where an offence was committed or where its consequences occurred. Cybercrime disrupts this model because the location of the offender, victim, computer system, data and financial transaction may all differ. Consider a hypothetical online banking fraud:

- the victim resides in Jaipur;
- the victim's bank account is maintained in Mumbai;
- the fraudster operates from another State;
- the command server is located in Singapore;
- the stolen funds are transferred through accounts in several jurisdictions; and
- the final proceeds are converted into cryptocurrency through an overseas exchange.

The question "where was the crime committed?" consequently has no simple answer.

Indian procedural law has begun to recognise this problem. Section 202 of the BNSS specifically addresses offences involving cheating through electronic communications and provides jurisdictional rules based upon locations connected to the communication and delivery or receipt of property. This reflects an attempt to adapt territorial jurisdiction to digital criminality. However, domestic jurisdictional rules cannot resolve situations in which relevant evidence or accused persons are located abroad. This creates a distinction between jurisdiction to prosecute and jurisdiction to obtain evidence. India may possess jurisdiction to prosecute an offence affecting an Indian victim while lacking unilateral authority to compel a foreign service provider to disclose data stored in another State. The distinction is fundamental because a criminal justice system may possess substantive jurisdiction over the offence but still be unable to obtain the evidence necessary to prove it.

 [ISSN 2581-5369]

VIII. India's Approach to International Cybercrime Frameworks: A Comparative Regulatory Perspective

The regulation of cybercrime has increasingly moved beyond the traditional objective of criminalising unauthorised access to computers and networks towards a broader regulatory model encompassing cybersecurity, intermediary responsibility, protection of digital infrastructure, electronic evidence, data governance and international cooperation. In this context, India's cybercrime framework can usefully be examined against the Budapest Convention on Cybercrime and the regulatory approaches developed by the European Union (EU), the United Kingdom (UK) and the United States (US).

A. India and the Budapest Convention: Substantive Convergence without Treaty Accession

The Convention on Cybercrime, commonly known as the Budapest Convention, represents the principal international framework for harmonising national cybercrime laws and facilitating cooperation in the investigation and prosecution of offences involving computer systems and electronic evidence. It addresses three interconnected areas: substantive criminal law, procedural powers for obtaining electronic evidence, and international cooperation.[33] India has not acceded to the Budapest Convention. Its position has historically been influenced by concerns regarding the Convention's negotiating history, India's absence from the original negotiating process, and questions concerning the adequacy of its mechanisms for transnational access to electronic data and mutual legal assistance. India has instead supported the development of a more universally negotiated international framework under the United Nations.

B. European Union: A Risk-Based and Systemic Regulatory Approach

The EU has developed one of the most comprehensive regulatory approaches to cybersecurity and digital governance. Unlike a model centred principally on criminal offences, the EU framework combines criminal-law cooperation with preventive cybersecurity regulation, data protection, platform governance and institutional supervision. A significant component is the NIS2 Directive (Directive (EU) 2022/2555).[34] NIS2 replaced the original NIS Directive and seeks to establish a higher and more harmonised level of cybersecurity across the Union. It

[33] Prashant Mali, *International Cybercrime Treaties and Case Laws: An Overview (Till December 2024)*, Cyber Law Consulting, https://www.cyberlawconsulting.com/global_cybersecurity_sco_framework.php (last visited Sept. 4, 2026).

[34] European Commission, *NIS2 Directive: Securing Network and Information Systems*, https://digital-strategy.ec.europa.eu/en/policies/nis2-directive (last visited Sept. 4, 2026).

 [ISSN 2581-5369]

expands the number of regulated sectors and entities, requires cybersecurity risk-management measures and introduces incident-reporting obligations. It also strengthens cooperation, supervision and enforcement mechanisms among Member States. The regulatory philosophy of NIS2 is particularly significant because it moves from a predominantly reactive model towards preventive regulation. Instead of waiting for a cyberattack to occur and then relying upon criminal law, regulated entities are expected to identify cybersecurity risks. The framework also gives greater importance to supply-chain security, vulnerability management and coordinated crisis response. This represents an important point of comparison for India. India's framework contains incident-response and reporting mechanisms, but the EU model places greater emphasis on imposing structured and continuing preventive duties upon organisations operating within designated sectors.

C. United Kingdom: Criminalisation Combined with Preventive Regulation

The UK follows a somewhat different model. Its regulatory structure combines a strong criminal-law foundation with sector-specific cybersecurity and online-safety regulation. The Computer Misuse Act 1990 (CMA) remains the principal legislation dealing with cyber-dependent crime. It criminalises unauthorised access, unauthorised acts intended to impair computer operations, serious damage caused through unauthorised acts, and the production or supply of articles intended for use in specified computer offences.[35] The UK has progressively amended and interpreted the CMA to accommodate technological developments. However, the UK regulatory approach is no longer confined to criminalisation. The Online Safety Act 2023, for example, imposes statutory duties upon regulated online services concerning illegal content. Providers are required to undertake risk assessment and adopt proportionate systems and processes to prevent or mitigate specified harms and to remove certain illegal content when they become aware of it.[36] This is significant when compared with India because it demonstrates how cyber regulation can evolve from a conventional computer-misuse statute towards a broader system of regulatory accountability.

D. United States: A Decentralised and Enforcement-Oriented Model

The US follows a more decentralised regulatory model than the EU. Rather than relying upon one comprehensive federal cybersecurity statute, the US framework consists of multiple federal statutes, sector-specific regulations, executive measures and state laws. The Computer Fraud

[35] Maria Grazia Porcedda, *Sentencing Data-Driven Cybercrime: How Data Crime with Cascading Effects Is Tackled by UK Courts*, 48 COMP. LAW & SECURITY REV. 1, 26 (2023), https://doi.org/10.1016/j.clsr.2023.105793.
[36] Hedvig Schmidt, *The Online Safety Act 2023*, 16 J. OF MEDIA LAW 202 (2024), https://doi.org/10.1080/17577632.2025.2459440.

 [ISSN 2581-5369]

and Abuse Act (CFAA), 18 U.S.C. § 1030, constitutes a central federal criminal-law instrument for prosecuting computer-related offences. The US Department of Justice describes the CFAA as an important federal statute for addressing cyber-based crimes.[37]

At the same time, the US has increasingly supplemented criminal enforcement with regulatory requirements directed towards cybersecurity preparedness and incident reporting. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) requires the Cybersecurity and Infrastructure Security Agency (CISA) to establish reporting requirements for covered entities concerning specified cyber incidents and ransom payments. The US therefore illustrates a distributed regulatory model: criminal law addresses malicious conduct, while specialised agencies and sectoral legislation address cybersecurity risks, critical infrastructure and incident reporting. An additional feature of the US approach is the effort to distinguish malicious conduct from legitimate cybersecurity research. In 2022, the Department of Justice revised its CFAA charging policy to clarify that good-faith security research should not ordinarily be prosecuted under the statute. The comparative analysis thus reveals that India should not simply copy another jurisdiction. Rather, India should identify common principles: technological neutrality, strong electronic-evidence powers, procedural safeguards, institutional expertise and international cooperation. These principles are more durable than technology-specific legislative provisions.

IX. Anomalies and Proposed Legal and Institutional Reforms

A number of weaknesses exist; five principal structural weaknesses are nevertheless of prime importance and are discussed below:

1. Fragmentation: Cybercrime law is distributed across multiple statutes and regulatory instruments. This can create uncertainty concerning which provision applies to a particular technological offence.
2. Evidentiary complexity: Although the BSA recognises electronic evidence, admissibility does not eliminate challenges concerning authenticity, integrity, attribution and chain of custody.
3. Territorial limitations: Domestic law cannot independently compel access to evidence physically or legally controlled by foreign entities.

[37] Adam M. Bossler, *Cybercrime Legislation in the United States*, in The Palgrave Handbook of International Cybercrime and Cyberdeviance 257, 274 (Thomas J. Holt & Adam M. Bossler eds., 2020), https://doi.org/10.1007/978-3-319-78440-3_3.

4. Institutional inequality: Central institutions have increasingly sophisticated cyber capabilities, but investigative capacity may vary considerably among States and local police units.
5. Technological acceleration: Emerging technologies may evolve faster than the legislative process. This is particularly evident in deepfakes, generative AI, autonomous systems and new forms of digital financial crime.

These weaknesses indicate that India's future cybercrime policy should not simply pursue an offence-by-offence legislative strategy. Instead, the legal framework should be based upon technological neutrality, procedural adaptability, institutional coordination and international interoperability. These weaknesses can be overcome by the reforms provided below:

1. Adoption of a comprehensive cybercrime policy framework: India would benefit from a consolidated national cybercrime policy that clearly identifies substantive offences; investigative powers; electronic-evidence procedures; institutional responsibilities; victim protection; intermediary cooperation; international cooperation; and emerging technology risks. Such a policy need not replace the IT Act or other legislation. Instead, it should clarify their interaction.
2. Strengthening digital evidence protocols: Nationally standardised protocols should be developed for seizure of digital devices; forensic imaging; hashing; metadata preservation; chain-of-custody documentation; cloud evidence; cryptocurrency evidence; and AI-generated or synthetic media. The objective should be to ensure consistency from the initial investigation through trial.
3. Expedited preservation of foreign data: India should strengthen mechanisms for rapid preservation of electronic evidence located abroad. Preservation is particularly important because investigators may require time to obtain formal disclosure through mutual legal assistance procedures. A preservation-first model could prevent destruction or routine deletion of relevant evidence while the formal legal process is undertaken.
4. Greater international cooperation: India should strengthen operational cooperation with foreign law-enforcement authorities and consider deeper engagement with international cybercrime frameworks. The Budapest Convention provides a useful benchmark because it integrates substantive criminalisation, procedural powers and international cooperation.

 [ISSN 2581-5369]

5. Capacity building: Cybercrime training should extend beyond specialised cybercrime units. Ordinary police officers, prosecutors and judges increasingly encounter electronic evidence. Basic digital-forensics literacy should therefore become an integral component of criminal-justice training. The I4C's National Cybercrime Training Centre provides an institutional basis for such capacity building.
6. Technology-neutral drafting: Cybercrime legislation should avoid excessive dependence upon specific technologies. For example, legislation should regulate unlawful synthetic impersonation or deceptive manipulation rather than defining an offence exclusively in terms of a particular AI model or deepfake software. Technology-neutral drafting would also increase legislative durability.
7. Victim-centred cybercrime enforcement: Cybercrime policy should recognise that financial loss is not the only consequence of digital offending. Victims may experience reputational damage; psychological distress; privacy violations; identity compromise; loss of employment; social stigma; and prolonged financial consequences. A comprehensive legal framework should therefore include accessible reporting, rapid financial intervention, victim notification and mechanisms for recovery of unlawfully transferred funds where possible.

X. Conclusion

Cybercrime represents a fundamental challenge to conventional assumptions concerning criminal law, jurisdiction and evidence. The increasing dependence of social and economic life upon digital infrastructures has simultaneously expanded the opportunities for cyber offending and increased the complexity of criminal investigation. India has responded through a progressively expanding legal and institutional framework. The IT Act, 2000 remains the principal specialised cybercrime legislation, while the BNS, BNSS and BSA have incorporated digital dimensions into substantive criminal law, criminal procedure and evidence. The establishment and expansion of the Indian Cyber Crime Coordination Centre further demonstrates an institutional shift toward coordinated national cybercrime enforcement.

The BSA's express recognition of electronic and digital records is particularly significant. Yet admissibility alone cannot solve the deeper problems of authenticity, attribution, integrity and chain of custody. Similarly, the existence of cybercrime offences does not guarantee effective prosecution when evidence is located outside India's territorial jurisdiction. Cybercrime therefore exposes a fundamental limitation of territorially organised criminal justice: the State may possess jurisdiction over the offence while lacking immediate practical access to the

 [ISSN 2581-5369]

evidence required to prove it. The Budapest Convention illustrates the importance of integrating substantive criminalisation with procedural powers and international cooperation. Its emphasis on electronic evidence and cross-border cooperation provides a useful comparative benchmark for India.

The study concludes that India's future cybercrime framework should not be constructed primarily through the continuous creation of individual offences. Instead, reform should focus on integration. Substantive criminal law, criminal procedure, electronic evidence, forensic investigation, institutional coordination and international cooperation must operate as interconnected components. A technologically neutral legislative approach is equally important. Cybercrime law that is tied excessively to specific technologies risks becoming obsolete. The law should instead focus on unlawful conduct, intent, harm and evidentiary reliability while allowing investigators and courts to apply established legal principles to new technological environments. Ultimately, effective cybercrime regulation requires a balance between security and liberty. Strong investigative powers must coexist with constitutional safeguards, privacy and procedural fairness. India's challenge is therefore not merely to create stronger cybercrime laws but to construct a coherent, adaptable and rights-compatible cybercrime governance architecture. Such an architecture would enable India to respond not only to existing forms of cybercrime but also to future developments involving artificial intelligence, synthetic media, autonomous systems, cryptocurrency and increasingly decentralised digital infrastructures.

*****

 [ISSN 2581-5369]