Page 715 - 727 **DOI:** *https://doi.org/10.63108/IJLMH.12910*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 5

2026

Reconstructing India's Cybercrime Law: The Bharatiya Nyaya Sanhita, 2023 and the Emerging Architecture of Digital Criminal Justice

REGOTI AJAY KUMAR* AND S S L SHYAM KISHORE P**

ABSTRACT

The rapid digitisation of economic, social and governmental activity in India has produced a corresponding expansion in the scale, sophistication and transnational character of cybercrime. The replacement of the Indian Penal Code, 1860 by the Bharatiya Nyaya Sanhita, 2023 marks a significant reconfiguration of substantive criminal law. This paper undertakes a doctrinal examination of the adequacy of the new Sanhita, read together with the Information Technology Act, 2000 and the Bharatiya Sakshya Adhiniyam, 2023, to address contemporary cyber threats. The research purpose is to evaluate whether the technology-neutral drafting of the Sanhita, the express inclusion of cyber-crimes within the organised-crime provision, and its extraterritorial reach supply a coherent and enforceable framework, or whether structural gaps persist in definition, evidence, jurisdiction and institutional capacity. The methodology is primarily doctrinal, drawing upon statutory text, parliamentary materials, leading Supreme Court authorities on electronic evidence and free speech, and comparative insights from international instruments. The findings indicate that while the Sanhita improves coverage of cyber-enabled fraud, stalking, forgery and syndicate-level activity, it does not create a dedicated cybercrime regime; dual charging with the Information Technology Act continues to generate interpretive friction; evidentiary certification requirements remain a frequent point of failure; and cross-border investigation continues to confront mutual-legal-assistance delays. The paper concludes that the Sanhita constitutes a meaningful incremental advance rather than a comprehensive solution, and that adequacy ultimately depends upon coordinated interpretation, enhanced forensic capacity, clearer guidance on emerging technologies such as deepfakes, and stronger institutional coordination between special cyber legislation and general criminal law.

Keywords: *Bharatiya Nyaya Sanhita 2023, Cybercrime, Information Technology Act 2000, Organised Crime, Electronic Evidence, Digital Arrest, Deepfakes, Extraterritorial Jurisdiction*

* Author is a Final-Year LL.B. Student at Aurora Deemed to be University, Bhongir, Telangana, India. ORCID: https://orcid.org/0009-0003-0963-6072

** Author is a Final-Year LL.B. Student at Aurora Deemed to be University, Bhongir, Telangana, India. ORCID: https://orcid.org/0009-0004-9914-1205

 [ISSN 2581-5369]

I. INTRODUCTION

Cybercrime has moved from a peripheral concern of specialist investigators to a central challenge for Indian criminal justice. Financial fraud executed through phishing and social engineering, large-scale data breaches, ransomware attacks on critical infrastructure, the non-consensual dissemination of intimate images, and the emerging use of generative artificial intelligence to create deepfakes for fraud or reputational harm illustrate the breadth of the threat landscape. The legislative response has long rested on two pillars: the specialised provisions of the Information Technology Act, 2000 and the general offences of the Indian Penal Code, 1860, applied by analogy or extension to digital conduct. The enactment of the Bharatiya Nyaya Sanhita, 2023, which replaced the Penal Code with effect from 1 July 2024, invites a fresh assessment of that dual structure.[1]

The research problem is whether the Sanhita, read with the Information Technology Act, which remains in force, and the new evidentiary code, supplies an adequate framework for the detection, investigation, prosecution and prevention of contemporary cybercrime. Adequacy is understood here not merely as the formal presence of penal provisions, but as the existence of a coherent body of norms that is technologically adaptable, jurisdictionally effective, evidentially workable and institutionally enforceable, while remaining consistent with the constitutional guarantees of privacy, free speech and due process.[2]

The existing literature has analysed the Information Technology Act extensively, together with the difficulties of applying colonial-era Penal Code provisions to digital facts. Far less sustained attention has been devoted to the post-2024 architecture as an integrated system. The gap is particularly visible in relation to the interaction between the organised-crime provision of the Sanhita and cyber syndicates, the practical operation of dual charging, the continued centrality of certification requirements for electronic evidence, and the capacity of the general criminal law to respond to AI-generated content.

The paper proceeds as follows. Part II outlines the methodological approach and the analytical framework employed. Part III examines the principal substantive provisions of the Sanhita relevant to cyber conduct and their relationship with the Information Technology Act. Part IV analyses organised crime, terrorism and syndicate-level cyber activity under the new code. Part

[1] NAT'L CRIME RECORDS BUREAU, MINISTRY OF HOME AFFAIRS, GOV'T OF INDIA, CRIME IN INDIA 2023 (2025); Bharatiya Nyaya Sanhita, No. 45 of 2023, § 1(2), Acts of Parliament, 2023 (India); Ministry of Home Affairs, Notification S.O. 850(E) (Feb. 23, 2024) (India) (appointing July 1, 2024 as the date on which the Sanhita, save section 106(2), came into force).

[2] Information Technology Act, No. 21 of 2000, §§ 43, 66, 66C–66F, Acts of Parliament, 2000 (India); Bharatiya Nyaya Sanhita, No. 45 of 2023, Acts of Parliament, 2023 (India).

 [ISSN 2581-5369]

V addresses evidentiary and investigative challenges under the Bharatiya Sakshya Adhiniyam and the Bharatiya Nagarik Suraksha Sanhita. Part VI considers emerging technological threats, including deepfakes and digital-arrest scams. Part VII evaluates institutional capacity and cross-border cooperation. Part VIII synthesises the findings on adequacy and offers recommendations. The conclusion returns to the research problem and restates the principal claims without introducing new material.

II. Methodology and analytical framework

A. Doctrinal orientation

The inquiry is principally doctrinal. It interprets the enacted text of the Bharatiya Nyaya Sanhita, the Information Technology Act, the Bharatiya Sakshya Adhiniyam and the Bharatiya Nagarik Suraksha Sanhita, together with the Statements of Objects and Reasons and relevant parliamentary debates where available. Judicial decisions of the Supreme Court of India on electronic evidence, free speech in the digital sphere and informational privacy supply the constitutional and interpretive backdrop.[3]

Comparative materials, including the Budapest Convention and the 2024 United Nations Convention against Cybercrime, are consulted not for transplantation but to identify functional benchmarks against which Indian provisions may be assessed. Policy literature and institutional reports are used to illuminate operational realities that pure textual analysis cannot capture, particularly forensic capacity and delays in mutual legal assistance.[4]

B. Scope and limitations

The paper focuses on the criminal-law dimension of cyber regulation. It does not attempt a comprehensive treatment of civil remedies, sectoral cybersecurity directives, or the full regulatory architecture of the Digital Personal Data Protection Act, 2023, although intersections with data-protection norms are noted where they affect criminal investigation or intermediary liability.[5]

---

[3] Information Technology Act, No. 21 of 2000 (India); Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63, Acts of Parliament, 2023 (India); Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, Acts of Parliament, 2023 (India); *see, e.g.*, *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India) (free speech online); *Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473 (India) (electronic evidence); *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India) (informational privacy).

[4] *See generally* JONATHAN CLOUGH, PRINCIPLES OF CYBERCRIME (2d ed. 2015); Susan W. Brenner, *Cybercrime Metrics: Old Wine, New Bottles?*, 9 VA. J.L. & TECH. 13 (2004); *see also* Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185; United Nations Convention against Cybercrime, G.A. Res. 79/243, annex (Dec. 24, 2024).

[5] Digital Personal Data Protection Act, No. 22 of 2023, Acts of Parliament, 2023 (India); Information Technology Act, No. 21 of 2000, § 79 (India).

 [ISSN 2581-5369]

The term "cybercrime" is employed in a functional sense that encompasses both cyber-dependent offences (those that can be committed only through information systems) and cyber-enabled traditional offences (fraud, intimidation, sexual offences and organised crime executed or amplified by digital means). This usage accords with the charging patterns observed in practice since the Sanhita came into force.[6]

C. Analytical criteria of adequacy

Adequacy is assessed against five interlocking criteria: (i) substantive coverage of contemporary cyber threats; (ii) coherence between the general criminal code and the special cyber statute; (iii) evidentiary workability under the new evidence code; (iv) jurisdictional effectiveness, especially in cross-border cases; and (v) institutional and forensic capacity to give practical effect to the formal norms. These criteria structure the subsequent analysis and the final assessment.[7]

III. Substantive coverage of cyber conduct under the Bharatiya Nyaya Sanhita

A. Absence of a dedicated cyber chapter and the logic of technology-neutral drafting

Unlike the Information Technology Act, the Bharatiya Nyaya Sanhita does not contain a dedicated chapter on cyber offences. Instead, it extends the reach of traditional offences to electronic and digital modes of commission through technology-neutral language and, in selected provisions, through express reference to electronic communication or records. This drafting choice has been defended as future-proofing: a statute that does not freeze its definitions around particular technologies is less likely to be rendered obsolete by rapid innovation. At the same time, the absence of specialised definitions leaves interpretive work to courts and investigating agencies and may produce uneven application across jurisdictions. The Statement of Objects and Reasons accompanying the Sanhita Bill spoke of making the criminal law relevant to the contemporary situation and of adding new offences of organised crime and terrorist acts, but it made no reference to technology-enabled crime and stopped short of creating a self-contained cyber code.[8]

---

[6] *See* Majid Yar, *The Novelty of "Cybercrime": An Assessment in Light of Routine Activity Theory*, 2 Eur. J. Criminology 407, 407–27 (2005), https://doi.org/10.1177/147737080556056; David S. Wall, Cybercrime: The Transformation of Crime in the Information Age (2007).

[7] *See generally* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1596–635 (2003), https://www.nyulawreview.org/wp-content/uploads/2018/08/NYULawReview-78-5-Kerr.pdf.

[8] Information Technology Act, No. 21 of 2000, §§ 43, 66, 66C–66F, 67–67B (India); Bharatiya Nyaya (Second) Sanhita, 2023, Bill No. 173 of 2023, Statement of Objects and Reasons ¶¶ 3–4 (India).

Technology neutrality is therefore both a strength and a limitation. It permits the Sanhita to absorb new modalities of offending without constant amendment. It does not, however, supply the detailed definitional scaffolding that specialised cyber legislation can provide for novel threats such as AI-generated content or sophisticated forms of ransomware-as-a-service.[9]

B. Cheating, personation and financial cyber fraud

Sections 318 and 319 of the Sanhita address cheating and cheating by personation. These provisions, read with the corresponding provisions of the Information Technology Act on identity theft and on cheating by personation using a computer resource, form the principal legal response to phishing, one-time-password fraud, fake investment schemes and related social-engineering attacks. The aggravated form of cheating that dishonestly induces the delivery of property, punishable under section 318(4) with imprisonment of up to seven years, is frequently invoked in high-value digital fraud cases.[10]

The dual applicability of the Sanhita and the Information Technology Act generates both opportunity and friction. Prosecutors commonly charge both sets of provisions in order to capture the cyber-specific element and the underlying dishonest inducement. The principle that a special law prevails over a general law continues to govern in appropriate cases, yet the precise boundary remains contested in practice and has produced divergent approaches at the trial level.[11]

In high-volume financial cyber fraud, the combination of the Sanhita's cheating provisions with the identity-theft and personation offences of the Information Technology Act allows prosecutors to present a complete narrative of both the technical modus operandi and the dishonest inducement. The practical difficulty lies in drafting charge sheets with sufficient specificity to survive scrutiny under the special-law principle while still capturing the full culpability of the accused.[12]

C. Stalking, voyeurism and gendered cyber harms

Section 78 of the Sanhita defines stalking in terms that expressly include monitoring a woman's use of the internet, e-mail or any other form of electronic communication. Section 77 addresses voyeurism and aligns in significant measure with the privacy-violation provision of the

[9] Bharatiya Nyaya Sanhita, No. 45 of 2023 (India); Information Technology Act, No. 21 of 2000 (India).
[10] Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 318(4), 319 (India); Information Technology Act, No. 21 of 2000, §§ 66C–66D (India).
[11] *Sharat Babu Digumarti v. Govt. of NCT of Delhi*, (2017) 2 SCC 18 (India) (holding that where section 67 of the Information Technology Act applies to obscene material in electronic form, the accused cannot also be proceeded against under section 292 of the Indian Penal Code, the special law prevailing over the general).
[12] Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 318–319 (India); Information Technology Act, No. 21 of 2000, §§ 66C–66D (India).

 [ISSN 2581-5369]

Information Technology Act. These provisions re-enact, in substantially the same terms, sections 354C and 354D of the Penal Code, inserted by the Criminal Law (Amendment) Act, 2013, and so continue rather than enlarge the statutory foundation for cyberstalking and non-consensual image-based abuse. Section 75 on sexual harassment may also be attracted by certain forms of online sexual remarks and unwelcome sexual communications.[13]

Despite this textual foundation, practical barriers to reporting, investigation and victim support remain substantial. Many survivors of online gender-based violence continue to encounter a delayed first response, inadequate digital-forensic capacity at the local level, and secondary victimisation during investigation. Statutory adequacy in this domain therefore cannot be measured solely by the presence of express electronic-monitoring language; it must also be assessed against the lived experience of complainants seeking redress.

D. Forgery, electronic records and the expanded definition of document

The forgery provisions of the Sanhita, particularly sections 335 to 338, of which sections 335 to 337 extend in terms to false electronic records, operate alongside the definition of "document" in the Bharatiya Sakshya Adhiniyam, which now expressly includes electronic and digital records. The combination consolidates rather than creates coverage: the Information Technology Act, 2000 had already amended the Penal Code to define "electronic record" and to bring false electronic records within the offences of making a false document and forgery, so courts had no need to apply the older definitions by analogy. The practical efficacy of these provisions nevertheless depends on the quality of digital forensic examination and on the proper certification of electronic evidence under the Adhiniyam.[14]

Deepfakes and other synthetically generated content raise additional questions of attribution and authenticity. While the forgery and defamation provisions can be pressed into service, the absence of specific legislative guidance on the treatment of AI-generated material leaves courts and investigators without clear statutory markers for *mens rea* and *actus reus* in cases involving synthetic media.[15]

---

[13] Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 75, 77, 78(1)(ii) (India); Information Technology Act, No. 21 of 2000, §§ 66E, 67, 67A & 67B (India); *cf.* Indian Penal Code, No. 45 of 1860, §§ 354A, 354C, 354D (India) (inserted by Criminal Law (Amendment) Act, No. 13 of 2013).

[14] Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 335–340 (India); Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 2(1)(d), 61–63 (India); *cf.* Indian Penal Code, No. 45 of 1860, §§ 29A, 463, 464 (India) (as amended by Information Technology Act, No. 21 of 2000, § 91 & sch. I).

[15] *See* Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 318–319, 336, 356 (India); Information Technology Act, No. 21 of 2000, §§ 66C–66E (India).

 [ISSN 2581-5369]

IV. Organised crime, terrorism and syndicate-level cyber activity

A. Section 111 and the explicit inclusion of cyber-crimes

Section 111 of the Sanhita constitutes one of the most consequential innovations for large-scale cyber offending. For the first time in central Indian criminal law, organised crime is defined and criminalised as a distinct offence, and the definition expressly includes cyber-crimes committed by a person or a group of persons acting in concert, whether as members of an organised crime syndicate or on behalf of such a syndicate, to obtain direct or indirect material benefit. The provision carries severe penalties: imprisonment for a minimum of five years, extending to life, and, where the offence results in the death of any person, death or imprisonment for life.[16]

The practical significance of section 111 lies in its capacity to shift the prosecutorial focus from isolated individual acts to the enterprise structure of phishing rings, ransomware groups, mule-account networks and cross-border fraud syndicates. Previously, organised-crime frameworks existed primarily under state special laws such as the Maharashtra Control of Organised Crime Act, 1999. The centralisation of a cyber-inclusive organised-crime offence is therefore a structural advance.[17]

B. Petty organised crime under section 112

Section 112 addresses petty organised crime and supplies a lower threshold for smaller gang-based operations that may not meet the full organised-crime definition but nonetheless operate through coordinated digital means. The provision is particularly relevant to networks of mule-account operators, low-level phishing cells and local digital-fraud gangs that facilitate larger transnational schemes.[18]

C. Terrorist acts and overlap with cyber terrorism

Section 113 of the Sanhita defines terrorist acts in broad terms and overlaps with the cyber-terrorism provision of the Information Technology Act. The dual regime requires careful prosecutorial judgment to avoid both the under-charging of serious attacks on critical information infrastructure and the dilution of the specialised safeguards that accompany certain special-law regimes.[19]

---

[16] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 111(1) & Explanation, § 111(2) (India).

[17] Maharashtra Control of Organised Crime Act, 1999, Maharashtra Act No. 30 of 1999 (India); *cf.* Bharatiya Nyaya Sanhita, No. 45 of 2023, § 111 (India).

[18] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 112 (India).

[19] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 113 (India) (the Explanation to which leaves it to an officer not below the rank of Superintendent of Police to decide whether a case is registered under section 113 or under the Unlawful Activities (Prevention) Act, 1967); Information Technology Act, No. 21 of 2000, § 66F (India); Unlawful Activities (Prevention) Act, No. 37 of 1967 (India).

 [ISSN 2581-5369]

D. Assessment of the organised-crime innovation

The inclusion of cyber-crimes within the organised-crime definition is a clear legislative advance. Whether it proves adequate in practice will depend on the quality of investigation into syndicate structures, the ability to secure financial intelligence and international cooperation, and the restraint with which the provision is invoked, so that ordinary cyber offences are not artificially elevated into organised-crime prosecutions without supporting evidence of an enterprise. Judicial development of the definition will be essential to prevent both under-use and over-use of the provision.[20]

V. Evidentiary and Investigative Architecture

A. Electronic evidence under the Bharatiya Sakshya Adhiniyam

The Bharatiya Sakshya Adhiniyam continues, with refinements, the certification regime for electronic records that had been developed under the Indian Evidence Act, 1872. The Supreme Court's insistence on mandatory compliance with the certification requirement remains the governing principle. In practice, incomplete or defective certificates, broken chains of custody and the failure to record hash values at the point of seizure continue to be among the most common causes of failure in cyber prosecutions.[21]

The transition from the Indian Evidence Act to the Adhiniyam did not fundamentally relax the certification requirement. Courts continue to treat the certificate as a condition of admissibility rather than a mere formality. This strict approach protects the integrity of electronic evidence but places a premium on the technical competence of investigating officers and forensic examiners at the earliest stages of a case.[22]

B. Procedural powers under the Bharatiya Nagarik Suraksha Sanhita

The procedural code supplies powers of search, seizure and production of documents and electronic devices, together with related investigative tools. Early interpretive questions have arisen concerning the precise scope of production orders directed at intermediaries and the interaction of those powers with the data-protection and intermediary-liability regimes.[23]

The intersection of the production powers under the Nagarik Suraksha Sanhita with the safe-harbour framework under section 79 of the Information Technology Act, and with the purpose-

[20] Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 111–113 (India).
[21] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63 (India); *Anvar P.V.*, (2014) 10 SCC 473; *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 (India).
[22] *Anvar P.V.*, (2014) 10 SCC 473; *Arjun Panditrao Khotkar*, (2020) 7 SCC 1; *see also* Bharatiya Sakshya Adhiniyam, No. 47 of 2023, § 63(4) (India).
[23] Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, §§ 94, 105, 185, 530 (India).

 [ISSN 2581-5369]

limitation and security obligations that the Digital Personal Data Protection Act will impose once its substantive provisions take effect, creates a complex compliance environment for intermediaries. Clearer guidance on the relative priority of these regimes in the investigative context would reduce uncertainty for both law-enforcement agencies and service providers.[24]

C. Capacity constraints and the human element of enforcement

Statutory adequacy is inseparable from institutional capacity. Many state cyber cells continue to face shortages of trained personnel, forensic laboratories and standardised protocols for the preservation of volatile digital evidence. First-responding officers frequently lack the specialised training necessary to secure devices and logs in a manner that will survive later judicial scrutiny.

Training deficits at the first-response stage are particularly damaging because electronic evidence is often volatile. A failure to isolate devices, record hash values or maintain an unbroken chain of custody can render subsequent expert examination futile. Capacity building is therefore not a secondary policy preference but a necessary condition for the formal evidentiary regime to function as intended.[25]

VI. Emerging technological challenges

A. Deepfakes and generative artificial intelligence

Deepfake technology poses distinctive challenges of proof and classification. Existing provisions on forgery, cheating, defamation and privacy offences can be pressed into service, yet none was drafted with synthetic media specifically in mind. The technology-neutral posture of the Sanhita permits interpretive adaptation, but the absence of legislative or authoritative guidance on the attribution of AI-generated content creates uncertainty for both investigators and courts.[26]

Deepfakes used for financial fraud may attract the cheating and personation provisions; those used to cause reputational harm may attract defamation; and those involving non-consensual intimate imagery may engage the voyeurism, privacy and obscenity provisions. The difficulty lies less in the formal availability of penal sections than in the proof of origin, the attribution of

[24] Information Technology Act, No. 21 of 2000, § 79 (India); *Shreya Singhal*, (2015) 5 SCC 1 (reading down section 79(3)(b)); Digital Personal Data Protection Act, No. 22 of 2023 (India).

[25] Bharatiya Sakshya Adhiniyam, No. 47 of 2023, §§ 61–63 (India); Rick Ayers, Sam Brothers & Wayne Jansen, Nat'l Inst. of Standards & Tech., U.S. Dep't of Com., Guidelines on Mobile Device Forensics (NIST Special Publication 800-101 Rev. 1, 2014), https://doi.org/10.6028/NIST.SP.800-101r1.

[26] *See* Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 318, 319, 336, 356 (India); Information Technology Act, No. 21 of 2000, §§ 66D, 66E (India).

 [ISSN 2581-5369]

mens rea to the human controllers of generative systems, and the rapid dissemination of synthetic content across platforms.[27]

B. Digital arrest scams and impersonation of authority

Digital-arrest scams, in which offenders impersonate law-enforcement or judicial authorities to extract funds or compel the disclosure of credentials, have emerged as a high-volume form of cyber-enabled fraud. These schemes typically engage the provisions on cheating, personation, criminal intimidation and, where syndicate structures are present, organised crime. The Supreme Court has taken *suo motu* cognisance of the phenomenon, directed the Central Bureau of Investigation to investigate such scams across the country, and issued directions on the freezing of mule accounts, the restoration of defrauded funds and inter-agency coordination, while asking an inter-departmental committee to examine a shared-liability and victim-compensation framework.[28]

The digital-arrest phenomenon illustrates both the adaptability of existing penal provisions and the limits of a purely reactive criminal-law response. Prevention and rapid fund-restoration mechanisms are as important as successful prosecution. The Court's engagement with bank-freeze protocols and compensation frameworks underscores the need for a multi-institutional rather than a purely penal strategy.[29]

C. Ransomware and attacks on critical infrastructure

Ransomware attacks engage multiple overlapping provisions: unauthorised access and damage under the Information Technology Act, extortion and criminal intimidation under the Sanhita, and, in appropriate cases, the organised-crime or terrorist-act provisions. The adequacy of the framework turns less on the existence of penal sections than on the speed of detection, the quality of incident response, and the ability to disrupt payment channels and affiliate networks that frequently operate across borders.[30]

Ransomware-as-a-service models further complicate attribution and prosecution. Affiliate structures, cryptocurrency payment rails and jurisdictions with limited cooperative capacity create investigative challenges that no domestic penal code can fully resolve in isolation.

---

[27] Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 77, 318–319, 356 (India); Information Technology Act, No. 21 of 2000, §§ 66C–66E, 67, 67A (India).

[28] Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 111, 318, 319, 351 (India); *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Crl.) No. 3 of 2025 (India) (orders of Oct. 17, 2025, Dec. 1, 2025 and Aug. 4, 2026).

[29] *In re Victims of Digital Arrest Related to Forged Documents*, Suo Motu Writ Petition (Crl.) No. 3 of 2025 (India) (order of Aug. 4, 2026).

[30] Information Technology Act, No. 21 of 2000, §§ 43, 66, 66F (India); Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 111, 113, 308, 351 (India).

 [ISSN 2581-5369]

International cooperation and financial-intelligence coordination are indispensable complements to the Sanhita and the Information Technology Act.[31]

VII. Institutional capacity and cross-border dimensions

A. Domestic institutional architecture

The Indian Cyber Crime Coordination Centre and the National Cyber Crime Reporting Portal constitute the principal central mechanisms for reporting, coordination and analysis. Their effectiveness depends on seamless integration with state police forces, financial intelligence units and sectoral regulators. Fragmentation of responsibility and uneven capacity at the state level remain persistent constraints.

Central coordination platforms can improve reporting and data aggregation, but they cannot substitute for competent first response and forensic examination at the state and district levels. The adequacy of the overall system is therefore determined by the weakest link in the enforcement chain.

B. Extraterritorial reach and mutual legal assistance

Section 1(5)(c) of the Sanhita expressly extends its application to any person outside India who commits an offence targeting a computer resource located in India. The clause is not new: it re-enacts clause (3) of section 4 of the Penal Code, inserted by the Information Technology (Amendment) Act, 2008, and parallels section 75 of the Information Technology Act. It remains a significant assertion of jurisdiction. Its practical utility, however, continues to be limited by the delays and dual-criminality requirements of mutual legal assistance processes, by foreign blocking statutes, and by the physical location of servers and data.[32]

Comparative experience under the Budapest Convention and the newer United Nations instrument illustrates both the potential and the persistent difficulties of international cybercrime cooperation. Domestic long-arm jurisdiction is necessary but not sufficient; it must be matched by efficient channels for evidence sharing and the transfer of offenders.[33]

C. Intersection with data protection norms

The Digital Personal Data Protection Act will introduce purpose limitation, security safeguards and individual rights that intersect with criminal investigation. Its substantive obligations are

[31] *See* Convention on Cybercrime, *supra* note 4, arts. 23–35; United Nations Convention against Cybercrime, *supra* note 4.

[32] Bharatiya Nyaya Sanhita, No. 45 of 2023, § 1(5)(c) (India); *cf.* Indian Penal Code, No. 45 of 1860, § 4 cl. (3) (India) (inserted by Information Technology (Amendment) Act, No. 10 of 2009); Information Technology Act, No. 21 of 2000, § 75 (India).

[33] Convention on Cybercrime, *supra* note 4; United Nations Convention against Cybercrime, *supra* note 4.

 [ISSN 2581-5369]

not yet operative: by a notification of 13 November 2025 under section 1(2) of the Act, issued with the Digital Personal Data Protection Rules, 2025, sections 3 to 17 (save section 6(9)) take effect eighteen months from that date. Once they apply, data fiduciaries who are also intermediaries under the Information Technology Act will face dual compliance obligations, although section 17(1)(c) exempts processing in the interest of the prevention, detection, investigation or prosecution of offences from most of those obligations. Investigative demands for data must nonetheless be calibrated against these protections if the overall framework is to remain coherent and rights-respecting.[34]

VIII. ADEQUACY ASSESSMENT AND RECOMMENDATIONS

A. Principal findings on adequacy

The analysis yields five principal findings. First, the Sanhita improves the formal coverage of cyber-enabled traditional offences through technology-neutral language and selected express references to electronic means. Second, the organised-crime provision supplies a powerful new tool against syndicate-level cyber activity that was previously available only under state special laws. Third, dual charging with the Information Technology Act remains both necessary and productive of friction, particularly where the special-law principle is unevenly applied. Fourth, evidentiary certification and forensic capacity constitute the most frequent points of practical failure. Fifth, emerging technologies such as generative artificial intelligence and deepfakes expose residual definitional and attributional gaps that technology-neutral drafting alone does not fully resolve.

B. Recommendations for coherence and capacity

Legislative and regulatory guidance should clarify the relationship between Sanhita offences and the provisions of the Information Technology Act so that dual charging is principled rather than opportunistic. Authoritative guidance on the treatment of AI-generated content under the forgery, cheating and defamation provisions would reduce interpretive uncertainty. Investment in standardised forensic protocols, the training of first responders and the expansion of certified laboratory capacity is essential if the evidentiary rules are to function as intended.

Mutual legal assistance processes require streamlining, including the exploration of executive agreements that reduce reliance on traditional treaty channels for urgent digital evidence. Finally, victim-centric mechanisms for the rapid restoration of funds in financial cyber fraud

[34] Digital Personal Data Protection Act, No. 22 of 2023, §§ 1(2), 4–14, 17(1)(c) (India) (commencement notification of Nov. 13, 2025); Digital Personal Data Protection Rules, 2025 (notified Nov. 13, 2025) (India); Information Technology Act, No. 21 of 2000, § 79 (India).

 [ISSN 2581-5369]

should be institutionalised and monitored for effectiveness. These measures would convert the formal advances of the Sanhita into practical improvements in the detection, prosecution and prevention of cybercrime.

IX. Conclusion

The research problem posed at the outset was whether the Bharatiya Nyaya Sanhita, 2023, read together with the Information Technology Act and the new evidentiary and procedural codes, supplies an adequate legal framework for contemporary cybercrime in India. The analysis demonstrates that the Sanhita marks a meaningful incremental advance. Technology-neutral drafting, express recognition of electronic modes in key offences, an express extraterritorial reach, and the inclusion of cyber-crimes within the organised-crime definition collectively strengthen the formal architecture. At the same time, the framework remains incomplete. Dual charging continues to generate friction; evidentiary certification remains a frequent point of failure; institutional capacity lags behind the sophistication of offenders; and emerging technologies such as deepfakes expose residual gaps that textual neutrality alone does not fill.

Adequacy, on the understanding adopted in this paper, is therefore partial. The Sanhita improves the tools available to investigators and prosecutors, yet those tools will realise their potential only through coordinated interpretation, sustained investment in forensic and human capacity, clearer guidance on novel technological vectors, and stronger mechanisms of cross-border cooperation. The constitutional values of privacy, free speech and due process must continue to discipline the expansion of investigative power. In that sense, the transition from the Penal Code to the Sanhita is best understood not as a completed reform but as a foundation upon which a more coherent, capable and rights-respecting system of cyber-criminal justice must still be built.

*****

 [ISSN 2581-5369]