CURRENT CYBER LAW FRAMEWORK IN INDIA AND GAPS WITH REGULATORY FRAMEWORK

-Pranav Pal[1], Dr. Saurabh Siddhartha[2]

ABSTRACT

India has emerged as one of the world's foremost digital economies, with close to 900 million internet users and an expanding reliance on digital infrastructure for commerce, governance, and civic engagement. This digital growth has been accompanied by a sharp rise in cybercrime, exposing deep-seated weaknesses in the country's legal and institutional architecture. The primary legislative instrument governing cyberspace—the Information Technology Act, 2000 and its 2008 Amendment—was conceived in a technological era vastly different from the present. India's criminal law landscape was further transformed in 2023 through three landmark codifications: the *Bharatiya Nyaya Sanhita, 2023* (BNS), replacing the Indian Penal Code, 1860; the *Bharatiya Nagarik Suraksha Sanhita, 2023* (BNSS), replacing the Code of Criminal Procedure, 1973; and the *Bharatiya Sakshya Adhiniyam, 2023* (BSA), replacing the Indian Evidence Act, 1872. While these reforms modernise certain procedural and evidentiary dimensions of cybercrime prosecution, significant structural gaps persist: definitional anachronisms that fail to capture emerging threat vectors, the absence of specialised adjudicatory mechanisms, inadequate cross-border enforcement capability, fragmented regulatory oversight, and insufficiently robust privacy safeguards. This assignment critically examines the existing statutory and regulatory architecture governing cyberspace in India, identifies its principal lacunae in light of the new criminal codes, and proposes a reform agenda informed by comparative experience from the European Union, the United States, and Singapore.

Keywords: cybercrime governance, digital privacy rights, regulatory fragmentation, transnational jurisdictional enforcement, cyberspace adjudication.

1. Introduction

India recorded approximately 900 million internet users in 2023, making it the second-largest online population globally (International Telecommunication Union [ITU], 2023).[3] This connectivity has unlocked transformative gains in e-commerce, digital payments, and public service delivery. Simultaneously, however, it has created an expansive attack surface for malicious actors. The National Crime Records Bureau (NCRB) documented 65,893 cybercrime cases in 2022—a 24.4 per cent increase over 2021—encompassing financial fraud, ransomware, data theft, and online harassment (NCRB, 2023).[4]

The legislative response to this challenge has been cumulative and reactive. The Information Technology Act, 2000 (IT Act), broadly modelled on the UNCITRAL Model Law on Electronic Commerce, 1996,[5] provided India's foundational framework for electronic commerce and cyber offences. Its 2008 Amendment expanded criminal liability and introduced institutional mechanisms such as CERT-In. Most recently, three new criminal codes—the BNS, BNSS, and BSA—came into force on 1 July 2024, replacing the Indian Penal Code, the Code of Criminal Procedure, and the Indian Evidence Act respectively (Ministry of Home Affairs [MHA], 2023).[6] These codes carry significant implications for cybercrime prosecution, digital evidence admissibility, and trial procedure.

---

[1] LL.M. Cyber and Security Law, ICFAI University, Dehradun

[2] Assistant Professor, Law, ICFAI University, Dehradun

[3] International Telecommunication Union (ITU). (2023). *Measuring digital development: Facts and figures 2023*. Geneva: ITU Publications. https://www.itu.int/itu-d/reports/statistics/facts-figures-2023/

[4] National Crime Records Bureau (NCRB). (2023). *Crime in India 2022*. New Delhi: Ministry of Home Affairs. https://ncrb.gov.in/en/crime-india-2022

[5] United Nations Commission on International Trade Law (UNCITRAL). (1996). *UNCITRAL Model Law on Electronic Commerce with Guide to Enactment*. New York: United Nations.

[6] Ministry of Home Affairs (MHA), Government of India. (2023). *The Bharatiya Nyaya Sanhita, 2023 (Act No. 45 of 2023); The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023); The*

Despite these legislative developments, scholars have consistently argued that India's cyber law architecture remains reactive, under-resourced, and institutionally fragmented (Prasad, 2022; Sinha & Mathur, 2021).[7] This assignment proceeds as follows: Section 2 surveys the existing statutory framework with emphasis on the new criminal codes; Section 3 maps the regulatory ecosystem; Section 4 identifies and analyses the principal gaps; Section 5 draws on comparative international experience; and Section 6 offers reform recommendations.

2. Existing Cyber Law Framework in India

2.1 The Information Technology Act, 2000 and Its 2008 Amendment

The IT Act, 2000 constitutes the *lex specialis* of Indian cyber law. It confers legal recognition on electronic records and digital signatures (Sections 3-16), governs electronic governance and certifying authorities (Sections 17-42), and prescribes civil and criminal liability for a broad range of cyber offences (Sections 43-74). The 2008 Amendment introduced provisions addressing identity theft (Section 66C), cheating by personation through computer resources (Section 66D), violation of privacy through capturing or transmitting intimate images (Section 66E), cyber terrorism (Section 66F), and child sexual abuse material (Section 67B). Section 66A, which had criminalised broadly defined offensive online communication, was struck down as unconstitutional in *Shreya Singhal v. Union of India*, AIR 2015 SC 1523, on grounds of unreasonable restriction on free speech (Supreme Court of India, 2015).[8]

The Act also establishes a quasi-judicial framework for civil disputes: Adjudicating Officers under Section 46 may award compensation in disputes involving losses up to INR 5 crore, while the Cyber Appellate Tribunal (CyAT) under Section 48 provides appellate review. Wide powers of interception, monitoring, and decryption in the interest of national security are conferred on the Central Government under Section 69—a provision consistently criticised for its breadth and limited judicial oversight (Datta, 2021).[9]

2.2 The New Criminal Codes and Their Implications for Cyber Law

The enactment of the three new criminal codes marks the most comprehensive overhaul of India's criminal justice system since independence, with significant downstream consequences for cyber law enforcement. The *Bharatiya Nyaya Sanhita, 2023* (BNS) replaces the Indian Penal Code and consolidates several cyber-enabled offences. Section 111 of the BNS addresses organised crime, with an expanded definition that expressly encompasses cybercrimes perpetrated by criminal syndicates. Section 303 criminalises theft of property including electronically stored data. Significantly, the BNS expands the definition of 'terrorist act' to expressly include cyberterrorism, supplementing the existing Section 66F of the IT Act (MHA, 2023).[4]

The *Bharatiya Nagarik Suraksha Sanhita, 2023* (BNSS), replacing the Code of Criminal Procedure, introduces procedurally significant reforms for cybercrime investigation and trial. Section 94 of the BNSS empowers courts and police officers to summon electronic records held by service providers. Section 105 permits recording of witness statements through audio-video means, facilitating the examination of geographically distant cyber witnesses. The BNSS also provides for virtual hearings through video conferencing, reducing logistical barriers in complex multi-jurisdictional cybercrime cases (Ministry of Law and Justice, 2023).[10]

The *Bharatiya Sakshya Adhiniyam, 2023* (BSA), replacing the Indian Evidence Act, 1872, substantially updates the admissibility framework for electronic evidence. Section 63 of the BSA retains the requirement of a certificate authenticating electronic records but introduces greater flexibility in authentication, addressing the procedural rigidity criticised in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 (Supreme Court of India,

Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023). Gazette of India. https://www.mha.gov.in

[7] Prasad, R. (2022). Revisiting India's IT Act: A critical appraisal. *Indian Journal of Law and Technology*, 18(1), 45-72; Sinha, A., & Mathur, P. (2021). Cybercrime legislation in India: Challenges and way forward. NUJS Law Review, 14(3), 88-112.

[8] Supreme Court of India. (2015). *Shreya Singhal v. Union of India*, AIR 2015 SC 1523; (2015) 5 SCC 1.

[9] Datta, A. (2021). Surveillance law and digital rights in India: Analysing Section 69 of the IT Act. *Economic & Political Weekly*, 56(14), 32-40.

[10] Ministry of Law and Justice, Government of India. (2023). *The Bharatiya Nagarik Suraksha Sanhita, 2023 (Act No. 46 of 2023)*. Gazette of India. https://legislative.gov.in

2020).[11] The BSA also explicitly recognises electronic stamps and signatures as admissible, strengthening the evidential foundation for prosecuting digital offences.

2.3 The Data Protection Regime

Data protection was historically governed by Section 43A of the IT Act and the Sensitive Personal Data or Information (SPDI) Rules, 2011. The Digital Personal Data Protection Act, 2023 (DPDP Act) substantially overhauled this regime, establishing a consent-based framework, delineating obligations for Data Fiduciaries, conferring rights of access, correction, erasure, and grievance redressal on Data Principals, and creating the Data Protection Board of India (DPBI) as the primary adjudicatory authority (MeitY, 2023).[12] Financial penalties under the Act can reach INR 250 crore for significant data breaches—a marked escalation from the prior regime.

3. The Regulatory Ecosystem

India's regulatory architecture for cyberspace is distributed across multiple institutions, reflecting the cross-sectoral nature of digital risk but simultaneously creating structural coordination difficulties.

CERT-In: Established under Section 70B of the IT Act, CERT-In functions as the national nodal agency for cybersecurity incident response. Its 2022 Directions require covered entities to report incidents within six hours of detection, maintain system logs for 180 days, and synchronise clocks with Government-approved NTP servers (CERT-In, 2022).[13] These Directions attracted criticism for imposing disproportionate compliance burdens on small enterprises and potentially enabling surveillance without adequate privacy safeguards (Internet Freedom Foundation [IFF], 2022).[14]

National Cyber Security Coordinator (NCSC): Operating under the National Security Council Secretariat, the NCSC provides policy-level coordination across ministries. India's National Cyber Security Policy, 2013 remains the foundational strategic document (MeitY, 2013),[15] though a substantially revised draft has remained unfinished for several years, creating a policy vacuum that critically hampers coherent national cyber strategy.

Sectoral Regulators: The RBI, SEBI, IRDAI, and TRAI each issue sector-specific cybersecurity directives, creating overlapping and at times conflicting mandates. The RBI's Master Directions on Digital Payment Security Controls (2021)[16] and SEBI's Cybersecurity and Cyber Resilience Framework (2019)[17] are prominent examples of this regulatory fragmentation.

---

[11] Supreme Court of India. (2020). *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1.

[12] Ministry of Electronics and Information Technology (MeitY). (2023). *The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023)*. Gazette of India. https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf

[13] CERT-In. (2022). *Directions under sub-section (6) of section 70B of the Information Technology Act, 2000 relating to information security practices, procedure, prevention, response and reporting of cyber incidents*. MeitY. https://www.cert-in.org.in

[14] Internet Freedom Foundation (IFF). (2022). *Analysis of CERT-In Directions 2022: Concerns for privacy, security and business*. New Delhi: IFF. https://internetfreedom.in/cert-in-directions-analysis/

[15] Ministry of Electronics and Information Technology (MeitY). (2013). *National Cyber Security Policy 2013*. New Delhi: Government of India. https://www.meity.gov.in/cy-security/national-cyber-security-policy-2013

[16] Reserve Bank of India (RBI). (2021). *Master Directions on Digital Payment Security Controls*. Mumbai: RBI. https://www.rbi.org.in/Scripts/BS_ViewMasDirections.aspx?id=12032

[17] Securities and Exchange Board of India (SEBI). (2019). Cybersecurity and cyber resilience framework for stock brokers / depository participants. *Circular No. CIR/MRD/DP/01/2019*. Mumbai: SEBI.

Indian Cyber Crime Coordination Centre (I4C): Established under MeitY in 2018, I4C coordinates law enforcement responses to cybercrime, administers the National Cybercrime Reporting Portal (cybercrime.gov.in), and operates the financial fraud helpline '1930' (MHA, 2023).[4]

4. Critical Gaps in India's Cyber Law and Regulatory Framework

4.1 Absence of Specialised Adjudicatory Mechanisms

Despite the BNSS's useful provisions for virtual hearings and audio-video recording, India still lacks dedicated cybercrime courts staffed by technically trained judicial officers. Cybercrime prosecutions continue to be conducted before conventional sessions courts whose presiding officers typically lack the competence to evaluate complex digital evidence, forensic reports, or questions of technical attribution. This knowledge deficit contributes to prolonged trials and low conviction rates. The Law Commission of India's 221st Report (2009) recommended the creation of technically equipped e-courts,[18] yet implementation remains negligible over a decade and a half later. The Cyber Appellate Tribunal, conceived as the appellate forum for civil disputes under the IT Act, has been non-functional since 2011 due to persistent vacancies in the Presiding Officer's post—a governance failure of considerable magnitude (Bhushan, 2022).[19]

4.2 Gaps in the New Criminal Codes in Relation to Cyber Offences

While the BNS, BNSS, and BSA represent important modernisation steps, they exhibit notable gaps when evaluated against contemporary cyber law demands. The BNS does not contain a standalone, comprehensive chapter on cybercrime; cyber-related offences are distributed across chapters on property, organised crime, and terrorism, generating definitional inconsistencies and prosecutorial uncertainty (Verma & Nair, 2024).[20] The BNS makes no specific provision for ransomware, cryptojacking, deepfakes, artificial intelligence-enabled fraud, or cryptocurrency-linked money laundering—each a major and growing category of cybercrime.

The BNSS, while introducing electronic summons and virtual hearings, does not articulate a dedicated protocol for the search and seizure of cloud-hosted data or for compelling foreign intermediaries to produce evidence stored on overseas servers (Ministry of Law and Justice, 2023).[8] The BSA's updated electronic evidence provisions are constructive, but the Act does not address the admissibility of metadata, geolocation data, or AI-generated evidence—categories increasingly central to cybercrime prosecutions.

4.3 Inadequate Data Privacy and Protection

Although the DPDP Act, 2023 is a structural advance, commentators have identified substantive shortcomings. First, the Act contains broad exemptions for State and Government data processing, raising the risk of institutionalised surveillance without adequate legal safeguards (Bhatia & Bhatt, 2023).[21] Second, unlike the EU's General Data Protection Regulation (GDPR), the Act does not incorporate a 'privacy by design' mandate requiring data protection to be embedded in systems from inception (European Parliament & Council, 2016).[22] Third, the DPBI is constituted entirely through Central Government appointment, undermining its institutional independence. Fourth, the Act is silent on algorithmic profiling, automated individual decision-making, and meaningful protections for children's data on social media platforms beyond a general parental consent requirement.

4.4 Cross-Border Jurisdictional Deficits

Cybercrime is quintessentially transnational, yet India's legal framework remains largely territorial. The IT Act does not provide a coherent extraterritorial jurisdiction framework, and India is not a signatory to the Budapest Convention on Cybercrime, 2001—the principal multilateral instrument for international cooperation in this domain (Council of

[18] Law Commission of India. (2009). *221st Report: Need for legislation to regulate electronic crime / Cyber Crime*. New Delhi: Government of India.

[19] Bhushan, P. (2022). The dormant Cyber Appellate Tribunal: A governance failure. *NUJS Law Review*, 15(1), 200-218.

[20] Verma, S., & Nair, R. (2024). New criminal codes and cyber offences: An appraisal. *Journal of Indian Law and Society*, 15(2), 112-135.

[21] Bhatia, G., & Bhatt, J. (2023). Analysing the Digital Personal Data Protection Act, 2023. *NALSAR Student Law Review*, 17(2), 1-28.

[22] European Parliament & Council of the European Union. (2016). *General Data Protection Regulation (EU) 2016/679*. Official Journal of the European Union, L 119, 1-88.

Europe, 2001).[23] India's network of Mutual Legal Assistance Treaties covers fewer than fifty countries, and requests routinely take twelve to twenty-four months to be actioned—rendering the mechanism ineffective for real-time investigations (Subramaniam, 2022).[24] Critically, neither the BNSS nor the BNS addresses this vacuum. Attacks originating from hostile state actors, cryptocurrency fraud routed through offshore platforms, and cloud-hosted evidence therefore remain practically beyond the reach of Indian law enforcement.

4.5 Outdated Definitions and Penal Asymmetries

The IT Act's definitional architecture has not been updated to reflect contemporary technological realities. The statutory definition of 'computer' under Section 2(1)(l) does not explicitly encompass smart devices, Internet of Things (IoT) nodes, or autonomous systems—creating uncertainty in the Act's application to modern attack surfaces (Verma, 2020).[25] The BNS, despite its breadth, does not cure these definitional gaps. A further anomaly lies in the sentencing framework: Section 43 of the IT Act imposes unlimited civil liability for unauthorised access, yet the corresponding criminal offence under Section 66 carries only three years' imprisonment—an asymmetry that distorts deterrence. The BNS strengthens penalties for organised cybercrime but does not rationalise the broader sentencing structure for individual cyber offenders.

4.6 Fragmented Regulatory Oversight

The multiplicity of regulators—CERT-In, I4C, NCSC, RBI, SEBI, TRAI, IRDAI, and NCIIPC—creates overlapping mandates, regulatory arbitrage, and coordination failures. There is no single empowered cybersecurity authority comparable to the UK's National Cyber Security Centre or the US Cybersecurity and Infrastructure Security Agency (CISA). The 2022 CERT-In Directions were issued without adequate inter-agency consultation and generated compliance conflicts with existing RBI and TRAI requirements, illustrating the structural dysfunction of the current model (IFF, 2022).[12] The DPDP Act adds yet another body—the DPBI—without consolidating these overlapping mandates.

5. Comparative Analysis and Lessons for India

A comparative survey of mature cyber law regimes yields instructive lessons for India. The EU's GDPR, 2016, widely regarded as the global gold standard for data protection, establishes extra-territorial applicability, mandatory Data Protection Impact Assessments, and the right to erasure—features India's DPDP Act partially mirrors but does not fully replicate (Voigt & von dem Bussche, 2017).[26] The EU's NIS2 Directive (2022) further mandates cybersecurity risk management obligations for critical infrastructure operators and harmonised incident reporting timelines—an approach India could usefully adopt for its own critical sectors.

The United States addresses cybercrime through the Computer Fraud and Abuse Act (CFAA) and sector-specific legislation, complemented by the NIST Cybersecurity Framework (NIST, 2018)[27] a voluntary risk management standard widely adopted by critical infrastructure operators. The US model of sector-specific legislation anchored to a central coordinating agency (CISA) offers a workable template for reforming India's fragmented regulatory landscape.

Singapore's Cybersecurity Act, 2018, designates Critical Information Infrastructure (CII) sectors and establishes a mandatory licensing framework for cybersecurity service providers administered by the Cyber Security Agency

---

[23] Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention), ETS No. 185*. https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185

[24] Subramaniam, V. (2022). Mutual legal assistance in cybercrime investigations: India's challenges. *Journal of Cyber Policy*, 7(1), 55-78.

[25] Verma, R. (2020). Definitional inadequacies in the Information Technology Act, 2000: A critical study. *Christ University Law Journal*, 9(1), 121-146.

[26] Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A practical guide*. Cham: Springer. https://doi.org/10.1007/978-3-319-57959-7

[27] National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical infrastructure cybersecurity, Version 1.1*. Gaithersburg, MD: NIST. https://www.nist.gov/cyberframework

(Cybersecurity Agency of Singapore, 2018).[28] India's NCIIPC performs an analogous protective function but lacks the statutory licensing authority and operational independence of Singapore's regulator—a gap that the recommendations below seek to address.

6. Recommendations

Based on the preceding analysis, the following legislative and regulatory interventions are recommended:

First, enact a standalone *Cybercrime Code* consolidating offences currently scattered across the IT Act and the BNS into a single, technologically current statute. The Code should expressly address ransomware, deepfakes, cryptojacking, AI-enabled fraud, and cryptocurrency crime, with technology-neutral definitions of 'computer', 'data', and 'electronic record'.

Second, establish *dedicated Cybercrime Courts* at the district level staffed by technically trained judicial officers, modelled on the Fast Track Special Courts framework used for POCSO cases. The BNSS's provisions for virtual hearings should be fully leveraged to reduce geographic and logistical barriers.

Third, strengthen the *DPDP Act* by incorporating privacy by design, mandatory Data Protection Impact Assessments, algorithmic accountability provisions, and genuine regulatory independence for the DPBI through parliamentary appointment of its members, drawing on the GDPR model.

Fourth, accede to the *Budapest Convention*, or at minimum negotiate bilateral real-time mutual assistance agreements with major cyber-origin states. The BNSS should be amended to provide a clear domestic legal basis for compelling the production of evidence stored by foreign cloud service providers.

Fifth, consolidate regulatory oversight under a *single empowered national cybersecurity authority* integrating the functions of CERT-In, I4C, and NCSC, eliminating the coordination failures inherent in the present multi-regulator model.

Sixth, amend the *BSA* to explicitly address the admissibility of metadata, geolocation data, cloud-extracted records, and AI-generated evidence, and to provide clear standards for their authentication and chain of custody.

7. Conclusion

India's cyber law framework, centred on the IT Act 2000 and complemented by the transformative new criminal codes—the BNS, BNSS, and BSA—and the DPDP Act, 2023, represents a foundational yet structurally incomplete architecture. The new criminal codes mark a watershed moment in India's legal modernisation: the BNS expands the reach of criminal law into organised cybercrime and cyberterrorism; the BNSS introduces technology-sensitive procedural reforms including virtual hearings and electronic summons; and the BSA substantially updates the admissibility framework for digital evidence. Yet significant gaps remain—definitional obsolescence, the absence of specialised cybercrime courts, weak cross-border enforcement, fragmented regulatory oversight, and the DPDP Act's structural limitations collectively constrain the framework's effectiveness. As India pursues a USD 1 trillion digital economy, the adequacy of its cyber law architecture will bear directly on investor confidence, the protection of citizens' rights, and national security. The reform agenda proposed in this paper—drawing on comparative experience from the EU, the United States, and Singapore—offers a coherent, rights-respecting, and technologically adaptive path forward.

[28] Cybersecurity Agency of Singapore. (2018). *Cybersecurity Act 2018 (Act 9 of 2018)*. Singapore: Attorney-General's Chambers. https://sso.agc.gov.sg/Act/CA2018