THE LEGALITES LEXSCRIPTA
ISSN 3108-2416 (ONLINE)
Editor-in-Chief: - Prof. (Dr.) Aryendu Dwivedi
Volume II Issue II (April-June) Page No.: - 173 to 191

INDIA'S LEGAL FRAMEWORK FOR REGULATING CYBERCRIMES: A STATUTORY AND CONSTITUTIONAL ANALYSIS

Author

Priyanshi Sareen

LL.B (Hons)

Amity Law School Noida,

Amity University Uttar Pradesh

Co-author

Dr. Tanya Narula Chaudhary

Assistant Professor of Law

Amity Law School Noida

Amity University Uttar Pradesh

ABSTRACT

The digital transformation of India has catalyzed an explosive proliferation of social media platforms, simultaneously engineering a volatile new frontier for complex, socio-technical cybercrimes. This dissertation critically evaluates India's evolving legal framework governing social media-driven digital offenses, focusing on the intricate interplay between the legacy Information Technology (IT) Act, 2000, and the historic overhaul of the criminal justice system via the newly enacted Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS), and Bharatiya Sakshya Adhiniyam (BSA).

Employing a doctrinal and comparative analytical methodology, the study investigates the definitional ambiguities, procedural frictions, and jurisdictional overlaps created by this fragmented, dual-structured legal ecosystem. The research exposes profound constitutional tensions, particularly evaluating how executive mandates such as the traceability clause

under the IT Rules 2021 conflict with the fundamental right to informational privacy and end-to-end encryption architecture.

Through comparative analysis with advanced international regulatory models, including the European Union's Digital Services Act (DSA) and the United Kingdom's Online Safety Act (OSA), the study highlights critical domestic deficits. These include the glaring absence of an

independent digital regulatory authority, severe infrastructural inadequacies in digital forensics, and crippling hurdles in cross-border law enforcement driven by India's non-participation in frameworks like the Budapest Convention.

Ultimately, the dissertation establishes that India's current reactive and fragmented legal posture is unsustainable. It advocates for the enactment of a comprehensive, unified Social Media Cybercrime Act, the establishment of an independent regulatory body, and a paradigm shift toward proactive algorithmic accountability to seamlessly balance national security imperatives with the inviolable digital rights of Indian citizens.

Keywords: Social Media Cybercrimes, Bharatiya Nyaya Sanhita, Intermediary Liability, Digital Rights, Platform Accountability.

I. Introduction

The exponential proliferation of information and communication technology has catalyzed a paradigm shift in human interaction, global commerce, and administrative governance, simultaneously birthing a highly complex, borderless ecosystem of digital criminality. Cyberspace, characterized by its decentralized architecture, inherent anonymity, and instantaneous global transmission capabilities, has fundamentally altered the nature, typography, and scale of crime.[1] India, possessing one of the world's largest, most rapidly expanding, and deeply penetrated digital populations, finds itself at the crucible of this socio-technical transformation. Consequently, the regulation of cybercrimes necessitates a legal framework that is dynamically adaptive to technological evolution, technically precise in its terminology, and rigorously sound in its constitutional foundations.

Historically, the Indian state's response to digital offenses was predominantly anchored in the Information Technology Act, 2000 (IT Act), an instrument initially conceived to facilitate electronic commerce and provide legal recognition to digital signatures, but which was subsequently amended to serve as a specialized penal statute.[2] However, the inadequacy of forcing novel, sophisticated digital offenses into the archaic, physically-oriented terminologies of the colonial-era Indian Penal Code (IPC), 1860, and the Code of Criminal Procedure (CrPC), 1973, exposed significant jurisprudential and procedural lacunae.[3] Law enforcement agencies and the judiciary frequently struggled with overlapping jurisdictions, evidentiary ambiguities, and a lack of procedural clarity regarding digital artifacts.

The year 2023 marked a watershed moment in Indian legal and constitutional history with the systemic, structural overhaul of its criminal justice architecture. The introduction of the Bharatiya Nyaya Sanhita, 2023 (BNS), the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS), and the Bharatiya Sakshya Adhiniyam, 2023 (BSA) explicitly integrated technological realities into substantive, procedural, and evidentiary law.[4]

[1] Mansi Sharma, "Critical Study of Cyber Crimes and Effectiveness of Cyber Laws as Deterrent" (Dissertation)
[2] The Information Technology Act, 2000 (Act 21 of 2000)
[3] The Indian Penal Code, 1860 (Act 45 of 1860); The Code of Criminal Procedure, 1973 (Act 2 of 1974)
[4] The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023)

II. Constitutional Foundations

The constitutional framework of India forms the unshakeable bedrock upon which the entire edifice of cyber jurisprudence and digital regulation is constructed. The adjudication of cybercrimes continuously necessitates a highly delicate and sophisticated balancing act between the state's legitimate, sovereign aim to maintain public order and national security, and the citizen's fundamental rights in the digital sphere.[5] As cyberspace becomes the primary medium for democratic participation, the Constitution's Part III provisions must be interpreted dynamically to protect citizens from both state overreach and private digital exploitation.

Article 19(1)(a) – Freedom of Speech and Expression in the Digital Age

Article 19(1)(a) of the Constitution guarantees every citizen the fundamental right to freedom of speech and expression, an entitlement that the judiciary has unequivocally extended to the digital domain. The landmark judgment in Shreya Singhal v. Union of India (2015) serves as the quintessential defense of digital free speech in contemporary Indian jurisprudence.[6]

The Court observed that terms like "annoying," "inconvenient," or "offensive" are highly subjective and do not constitute recognized grounds for restricting speech under the Constitution, thereby generating an unconstitutional "chilling effect" on legitimate online discourse and political dissent. Shreya Singhal entrenched the absolute principle that mere public annoyance or administrative inconvenience cannot serve as a rationale for criminalizing digital speech, establishing a high threshold for state intervention in online expression.

Article 19(2) – Reasonable Restrictions and their Application to Online Speech

While Article 19(1)(a) robustly protects online expression, constitutional jurisprudence dictates that this right is not absolute. Article 19(2) permits the state to impose "reasonable restrictions" on the exercise of free speech in the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign states, public order, decency, or morality, or in relation to contempt of court, defamation, or incitement to an offense.

[5] Balancing Privacy and Security: Constitutional Implications in the Era of Cyber Crime", IJIRL (2025)
[6] Shreya Singhal v. Union of India, AIR 2015 SC 1523.

However, the judiciary has strictly mandated that any restriction must pass the test of proportionality. It must be proximately connected to the specified grounds a concept often referred to as the "spark in a powder keg" test for incitement. Regulations cannot be excessively broad or preemptive in a manner that suffocates lawful speech. Therefore, laws governing content takedowns, internet shutdowns, and the blocking of digital resources must be narrowly tailored to address a specific, imminent harm, preventing authoritarian state overreach in digital surveillance.

Article 21 – Right to Privacy, Right to be Forgotten, and Right to Internet Access

The evolutionary trajectory of Article 21 (Protection of Life and Personal Liberty) has profoundly and permanently shaped Indian cyber law. The unanimous nine-judge Constitution Bench decision in Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) formally and irrevocably recognized the Right to Privacy as an intrinsic, fundamental component of Article 21.[7] Puttaswamy transcended traditional physical notions of privacy, establishing informational privacy and data autonomy as fundamental rights. The Court established a rigorous, four-fold proportionality test for any state action or legislation infringing on digital privacy: (i) legality (existence of a valid law), (ii) legitimate aim (necessity of the state action), (iii) rational nexus (proportionality between the aim and the means), and (iv) necessity (the implementation of the least restrictive measure).[8] This right is not absolute; courts frequently engage in a complex balancing act, weighing the individual's right to digital erasure against the public's right to information, historical accuracy, and the preservation of judicial records.[9]

Furthermore, the right to access the internet itself has been elevated to a quasi-fundamental status. In cases such as Anuradha Bhasin v. Union of India (2020) and the Kerala High Court's ruling in Faheema Shirin, the judiciary recognized that internet access is an indispensable enabler of the fundamental rights guaranteed under Articles 19 and 21. These judgments established that indefinite internet suspensions and arbitrary digital blackouts are unconstitutional, demanding that any restriction on internet infrastructure must be temporary, necessary, and strictly proportionate to a legitimate state emergency.[10]

[7] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
[8] The Puttaswamy Test: Right to Privacy", LiveLaw (2024)
[9] Right to be Forgotten: The Ongoing Battle Between Privacy and the Internet's Memory", Legal 500 (2024)
[10] Anuradha Bhasin v. Union of India, (2020) 3 SCC 637

Article 14 – Equality Before Law and Equal Protection in Cybercrime Prosecution

Article 14 of the Constitution guarantees equality before the law and equal protection of the laws within the territory of India, serving as the primary bulwark against arbitrary and discriminatory state action. In the contemporary, technologically advanced landscape of cybercrime investigation, this article assumes immense significance due to the increasing deployment of algorithmic tools, Artificial Intelligence (AI), and machine learning by law enforcement agencies.

Police forces are increasingly utilizing algorithmic systems for predictive policing, digital surveillance, pattern detection, and suspect identification.[11]While these technologies promise enhanced investigative efficiency, they raise profound Article 14 concerns regarding algorithmic bias and systemic discrimination. Machine learning models are trained on historical crime data; if this underlying data reflects historical prejudices related to caste, religion, gender, or socio-economic status, the algorithm inherently risks codifying and reproducing these biases at scale.

The opaque, "black-box" nature of algorithmic decision-making fundamentally conflicts with the constitutional requirement of procedural fairness, transparency, and non-arbitrariness. If predictive policing tools disproportionately profile specific demographic or marginalized groups for intensive digital surveillance or preemptive cyber-investigation, they violate the standard of reasonable classification required by Article 14. Consequently, legal scholars and constitutional experts argue that the current deployment of AI in cyber policing operates in a highly unregulated constitutional grey zone. To satisfy Article 14, there is an urgent jurisprudential need for statutory safeguards that ensure algorithmic transparency, regular bias auditing, and strict accountability mechanisms in digital law enforcement.

Article 51A(j) – Fundamental Duty to Promote Scientific Temper and Responsible Use of Technology

Part IVA of the Constitution, specifically Articles 51A(h) and 51A(j), articulates the fundamental duties of citizens to develop a "scientific temper, humanism and the spirit of inquiry and reform," and to "strive towards excellence in all spheres of

[11] Pratyaksh Joshi and Yogesh Wamankar, "Algorithmic Policing and Due Process in Cybercrime Investigations: A Constitutional Analysis", 2 Shodh Samajik 57 (2025)

individual and collective activity". While fundamental duties are inherently non-justiciable and cannot be enforced directly through court writs, they have been consistently interpreted by the judiciary as moral imperatives that guide public policy, statutory interpretation, and civic behavior.

In the context of cyber law and digital society, the constitutional mandate to develop a scientific temper translates directly into an obligation for responsible digital citizenship and digital hygiene. It imposes a collective civic responsibility on the populace to engage with technology ethically, to critically evaluate digital information to curb the viral spread of deepfakes, misinformation, and cyber-propaganda, and to abstain from participating in or enabling cybercrimes. The judiciary occasionally invokes these duties to uphold the validity of state regulations aimed at fostering a safe, secure, and critically literate digital environment, positing that the enjoyment of digital rights is inextricably linked to the performance of digital duties.[12]

III. Information Technology Act, 2000 and Its Amendments

The Information Technology Act, 2000 (IT Act) remains the foundational, specialized statutory legislation governing digital interactions, electronic commerce, and cyber offenses in the Republic of India. Originally enacted in the dawn of the internet era to provide legal recognition to electronic records, validate digital signatures, and facilitate e-commerce, the statute underwent massive transformations, particularly through the IT (Amendment) Act, 2008. These amendments fundamentally shifted the Act's center of gravity, transforming it into a robust, comprehensive penal framework designed to address an escalating array of complex cyber threats.

Scheme and Objectives of the IT Act 2000

The IT Act adopts a bipartite approach to digital misconduct, bifurcating offenses into civil contraventions and criminal offenses. Civil contraventions, such as unauthorized access or corporate data breaches leading to financial loss, are adjudicated by specialized Adjudicating Officers who possess quasi-judicial powers to levy heavy financial penalties and award compensation. Conversely, criminal offenses involving mens rea (criminal intent) such as cyber terrorism, child pornography, and identity

[12] The Constitution of India, art. 51A(h) & (j)

theft are investigated by law enforcement agencies and prosecuted in criminal courts, attracting severe custodial sentences.

Key Provisions Relevant to Social Media and Cybercrimes

The substantive penal provisions of the IT Act are primarily clustered in Chapter XI. The following table provides an exhaustive breakdown of the critical sections governing modern cybercrimes:

1. Section 43 & 66 Damage to Computer Resources & Computer-Related Offenses
2. Section 43 prescribes civil financial penalties for unauthorized access, downloading data, introducing viruses, or causing denial of service.
3. Section 66 elevates these exact acts to criminal offenses if committed "dishonestly" or "fraudulently," bridging the gap between civil liability and criminal culpability.
4. Section 66A Punishment for Offensive Online Messages This provision penalized the sending of information that was "grossly offensive" or had a "menacing character." It was struck down entirely by the Supreme Court in Shreya Singhal (2015) for violating Article 19(1)(a) due to unconstitutional vagueness and the chilling effect it imposed on free speech.
5. Section 66C Identity Theft Penalizes the fraudulent or dishonest use of another person's electronic signature, password, or any other unique identification feature. This is the primary tool against credential stuffing and account takeovers.
6. Section 66D Cheating by Personation Targets phishing attacks, social engineering scams, and digital impersonation where a computer resource or communication device is utilized to deceive an individual.
7. Section 66E Violation of Privacy Criminalizes the intentional capturing, publishing, or transmitting of images of a person's private areas without their explicit consent, serving as a vital tool against voyeurism and non-consensual image sharing.
8. Section 66F Cyber Terrorism Addresses acts intended to threaten the unity, integrity, security, or sovereignty of India through digital means. This includes attacking Critical Information Infrastructure (CII) or gaining unauthorized access to sensitive state data.

9. Section 67 penalizes the digital transmission of obscenity.
10. Section 67A addresses material containing sexually explicit acts.
11. Section 67B specifically targets the browsing, creation, and distribution of Child Sexual Abuse Material (CSAM), aligning with global child protection mandates.
12. Section 69 Power to Intercept, Monitor, and Decrypt Grants expansive executive powers to the Central and State Governments to intercept or decrypt any digital information passing through a computer resource, strictly in the interest of national security and public order.
13. Section 69A Blocking of Websites and Content Authorizes the government to issue directions to intermediaries for blocking public access to specific websites or content that threatens state sovereignty or public order. The constitutionality of this section was upheld due to its embedded procedural safeguards.
14. Section 79 Safe Harbour Immunity for Intermediaries Grants conditional legal immunity to network service providers, ISPs, and social media platforms, shielding them from liability for third-party content, provided they act merely as passive conduits and observe prescribed due diligence.

IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

To operationalize the "due diligence" requirements mandated by Section 79 for retaining safe harbour immunity, the government promulgated the IT Rules, 2021. These rules represent a paradigm shift in platform regulation, moving from a passive notice-and-takedown regime to a framework of proactive compliance and stringent platform accountability. [13]

Significant Social Media Intermediaries (SSMIs) Obligations:

The rules introduced a tiered regulatory structure, creating a specific classification known as Significant Social Media Intermediaries (SSMIs) defined as platforms boasting over 5 million registered Indian users. Recognizing their disproportionate influence on public discourse, SSMIs face heavy compliance burdens. They are mandated to physically appoint three key personnel resident in India: a Chief Compliance Officer (personally liable for the platform's failure to observe due

[13] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, r. 4

diligence), a Nodal Contact Person (available 24/7 for coordination with law enforcement agencies), and a Resident Grievance Officer. Additionally, SSMIs must publish monthly compliance reports detailing the volume of grievances received and the proactive actions taken, and they must deploy automated technological tools to proactively identify and remove CSAM and content depicting rape.

Traceability Clause and Constitutional Tension with Privacy

The most fiercely contested provision of the IT Rules 2021 is Rule 4(2), commonly referred to as the "traceability clause." This rule mandates that SSMIs providing messaging services must possess the technological capability to identify the "first originator" of information on their platforms, specifically for investigating severe offenses related to state security, public order, or sexual violence.

This requirement has generated immense constitutional friction. Platforms operating on end-to-end encryption (E2EE), such as WhatsApp and Signal, argue that traceability is mathematically and architecturally incompatible with E2EE. To comply, intermediaries would be forced to re-engineer their architecture to maintain a pervasive, permanent record of every message sent, or inject cryptographic "fingerprints" into all communications, thereby creating a mass surveillance apparatus. Legal scholars and civil liberties advocates argue that Rule 4(2) violates the Puttaswamy proportionality test. They contend that breaking encryption which protects the financial, personal, and professional communications of hundreds of millions of innocent citizens merely to trace a minuscule fraction of criminal actors constitutes a grossly disproportionate invasion of the fundamental right to informational privacy and anonymity, effectively destroying the digital presumption of innocence.

Grievance Redressal Mechanisms and Government Oversight

The 2021 Rules mandate robust internal grievance redressal mechanisms, requiring platforms to acknowledge user complaints within 24 hours and resolve them within 15 days. Addressing instances of platform unresponsiveness, the 2023 amendments to the rules introduced government-appointed Grievance Appellate Committees (GACs). These GACs serve as an alternative appellate body, allowing users to appeal content moderation decisions made by the platforms directly to a government panel. While this increases platform accountability, media watchdogs have raised concerns

regarding the independence of these committees and the potential for increased government oversight over digital content moderation.

IV. Bharatiya Nyaya Sanhita, 2023 (BNS) – Cybercrime Provisions

On July 1, 2024, the Indian criminal justice system experienced a structural metamorphosis as the Bharatiya Nyaya Sanhita, 2023 (BNS) officially repealed and replaced the 163-year-old Indian Penal Code (IPC), 1860. Enacted during the British colonial administration, the IPC was conceptualized in a purely analog era. It relied heavily on strained, expansive judicial interpretations to prosecute digital crimes, utilizing terminology rooted entirely in physical, structural paradigms (e.g., treating electronic data manipulation under physical trespass or physical document forgery).
The BNS, conversely, was engineered from its inception to be "technology-neutral" and future-ready. It systematically modernizes statutory language, explicitly integrating electronic communications, digital records, and digital devices into the functional scope of substantive criminal liability. Rather than segregating cybercrimes into a quarantined, dedicated chapter, the legislative drafting of the BNS weaves digital modalities seamlessly throughout traditional offenses against the human body, property, and the state.

Provisions Directly Applicable to Social Media and Cybercrimes

1. Section 111 – Organised Crime (Cyber-Enabled): This represents a monumental statutory addition. Section 111 creates a specific offense for "organised crime" committed by a crime syndicate, explicitly including "cyber-crimes" within its definitional ambit. Previously, cybercrimes were largely treated as isolated offenses. Section 111 empowers law enforcement to aggressively prosecute transnational phishing rings, ransomware syndicates, digital extortion networks, and large-scale financial fraud operations as organized criminal enterprises. This enables the prosecution of not just the technical perpetrators, but also the financiers, masterminds, and facilitators, imposing stringent penalties that extend to life imprisonment or death, coupled with massive financial fines.
2. Section 113 – Terrorist Acts via Digital Means: Responding to the asymmetric realities of modern warfare and terrorism, Section 113 provides a

comprehensive definition of terrorist acts. It penalizes actions intending to threaten the unity, integrity, and economic security of India, or intimidate the general public. The utilization of cyber infrastructure to launch debilitating attacks against national grids, telecommunication networks, or public transportation systems now falls unequivocally under this severe penal provision, bringing general criminal law into alignment with specialized anti-terror statutes.

3. Section 152 – Acts Endangering Sovereignty (The Sedition Replacement): Section 152 replaces the historically contentious and archaic offense of sedition (former Section 124A IPC). It penalizes acts that purposely or knowingly excite secession, armed rebellion, subversive activities, or endanger the sovereignty, unity, and integrity of India. Crucially, the provision explicitly criminalizes such acts when committed "through electronic communication" or by financial means. While the government asserts this removes the colonial stain of "sedition," legal scholars point out that the language remains exceptionally broad. Terms like "subversive activities" lack precise statutory definitions, raising apprehensions that the provision could be weaponized to criminalize legitimate online political dissent, journalistic critique, or digital activism, thereby recreating the chilling effect on free speech.
4. Section 196 & 197 – Promoting Enmity and Prejudicial Assertions Online: Corresponding to the former IPC Sections 153A and 153B, these provisions have been expressly modernized. Section 196 penalizes the promotion of disharmony on grounds of religion, race, or language, while Section 197 penalizes assertions prejudicial to national integration. Both sections have been updated to explicitly include acts committed "through electronic communication". Furthermore, Section 197(1)(d) is a vital new addition that specifically targets the digital dissemination of "false or misleading information" (fake news) that jeopardizes national sovereignty or security, providing a direct statutory mechanism to combat digital disinformation campaigns.
5. Section 351 – Criminal Intimidation via Electronic Messages: By incorporating the phrase "in any manner" into the definition of criminal intimidation, Section 351 explicitly subsumes digital threats. This allows

prosecutors to seamlessly apply severe penal sanctions against cyberstalking, online death threats, doxxing, and intimidation executed via emails, social media comments, or encrypted messaging platforms.

6. Section 318 – Cheating and Online Fraud: Serving as the bedrock provision for prosecuting the explosive growth of digital financial crimes, Section 318 modernizes the traditional offense of cheating. It provides the primary legal avenue for prosecuting modern vectors of financial deception, including Unified Payments Interface (UPI) frauds, crypto-investment scams, advance-fee frauds, and the establishment of fraudulent e-commerce portals, carrying punishments of up to seven years imprisonment.
7. Section 303 – Theft of Electronic Data: Under the legacy IPC, the offense of theft (Section 378) rigidly required the moving of "movable property." The Supreme Court historically grappled with whether intangible digital data qualified as movable property capable of being stolen. While the IT Act (Section 43) addressed data theft through civil penalties, the BNS modernizes the conceptual framework of property offenses. By defining "document" and integrating electronic records into the penal code, the BNS facilitates the prosecution of data theft, corporate espionage, and unauthorized data exfiltration as substantive property crimes.
8. Section 79 – Assault or Criminal Force to Woman through Digital Medium: Section 79 represents a critical, gender-centric advancement in Indian cyber law. It penalizes any word, gesture, or act intended to insult the modesty of a woman. Evolving beyond the requirement of physical proximity or physical assault found in older laws, Section 79 extends robust legal protections into the digital realm. It covers non-verbal online misconduct, targeted virtual abuse, sending unsolicited explicit imagery, and digital sexual harassment, reflecting an updated understanding of modern societal challenges regarding women's digital safety.
9. Section 69 – Sexual Intercourse through Deceit (The Digital Grooming Angle): Section 69 introduces a novel, highly debated offense penalizing sexual intercourse obtained by deceitful means or the false promise of marriage, distinct from the offense of rape. In the context of cyberspace, this provision holds profound implications for addressing "digital grooming," catfishing, and predatory behavior on online dating platforms and matrimonial

websites. It targets perpetrators who actively suppress their true identity or employ deceptive electronic inducements to secure physical intimacy. However, legal practitioners caution that this section presents immense evidentiary complexities. Differentiating criminal deceit orchestrated from the inception of a digital interaction from a mere breakdown of a consensually initiated virtual relationship requires rigorous, complex digital forensic evidence to establish intent.

10. Defamation: The BNS retains and updates the provisions on defamation, explicitly recognizing that digital publications, retweets, and social media posts possess an amplified, viral capacity to damage an individual's personal and professional reputation instantaneously and permanently.

V. Analysis: Improvements over IPC and Remaining Gaps

The BNS represents a monumental, indispensable leap in textual modernization. It ensures that public prosecutors and trial court judges are no longer forced to rely on strained, analogical interpretations of 19th-century physical statutes to prosecute 21st-century digital syndicates. The explicit inclusion of electronic communications across offenses ensures greater legal certainty.

However, critical gaps and architectural challenges persist. Foremost is the issue of regulatory overlap. The BNS operates concurrently with the IT Act. Conduct such as digital obscenity or data theft is punishable under both the BNS and specific sections of the IT Act. Without strict statutory harmonization or clear overriding clauses, this concurrency creates redundant regulatory regimes, subjects defendants to multiple overlapping charges for a single digital act, complicates trial procedures, and increases the compliance burden on digital platforms. Furthermore, while Section 111 includes cybercrime as organized crime, the lack of a granular, self-contained definition of "cyber-crime" within the BNS itself may lead to varied judicial interpretations across different state jurisdictions.

VI. Other Relevant Legislation

Beyond the foundational penal Sanhitas and the IT Act, the regulation of cybercrimes in India operates within a complex, interlocking matrix of specialized auxiliary legislations that address highly specific digital harms, vulnerable demographics, and data governance.

Protection of Children from Sexual Offences (POCSO) Act, 2012

The POCSO Act works in tandem with the IT Act to relentlessly combat online offenses against minors. The global proliferation of digital Child Sexual Abuse Material (CSAM), digital grooming, and the live-streaming of abuse are critical law enforcement priorities. A unique and powerful feature of POCSO is Section 30, which institutes a statutory presumption of a culpable mental state. In digital investigations, if a suspect is found possessing, downloading, or distributing CSAM on their devices, the legal burden shifts heavily to the accused to prove the absence of criminal intent. This reverse-burden mechanism is a highly effective legal tool in prosecuting and dismantling dark-web child exploitation networks, where proving explicit intent is often technologically difficult.[14]

Indecent Representation of Women (Prohibition) Act, 1986 (IRWA)

Enacted in a pre-internet era, IRWA was originally intended to ban the derogatory and indecent depiction of women in print media, publications, and physical advertisements.

Digital Personal Data Protection Act, 2023 (DPDPA)

Rooted entirely in the Puttaswamy constitutional privacy mandate, the DPDPA 2023 establishes India's first comprehensive, cross-sectoral data governance framework. It imposes strict obligations on Data Fiduciaries regarding transparent notice, explicit user consent, and strict purpose limitation. However, the DPDPA's intersection with cybercrime investigation is defined heavily by Section 17(1)(c). This section grants sweeping exemptions from these privacy obligations when the processing of personal data is deemed necessary for the "prevention, detection, investigation or prosecution of any offence".

While this exemption is undeniably crucial for ensuring that privacy laws do not cripple rapid police action during time-sensitive cyber-investigations, privacy advocates and legal scholars warn of its risks. They argue that the broad, un-nuanced phrasing of Section 17(1)(c) which lacks the explicit proportionality requirements and judicial oversight mechanisms found in equivalent EU privacy legislation risks

[14] The Protection of Children from Sexual Offences Act, 2012 (Act 32 of 2012), s. 30

facilitating unchecked state surveillance and the unauthorized sharing of personal citizen data among disparate government agencies under the guise of crime prevention.[15]

The Press and Registration of Periodicals (PRP) Act, 2023

Modernizing archaic media law, the PRP Act entirely replaces the colonial-era Press and Registration of Books Act, 1867. Governed by the newly designated Press Registrar General of India (PRGI), the Act implements an entirely digital, streamlined registration framework via the Press Sewa Portal. Crucially, the accompanying rules mandate that digital news publishers must upload the exact electronic facsimiles of their physical publications to government portals within 48 hours. This brings digital news dissemination under a structured, national regulatory mechanism. Upholding the ethos of press freedom, the Act substantially decriminalizes minor procedural lapses removing the threat of imprisonment for administrative errors while simultaneously demanding strict digital accountability and continuous publication verification.

Cyber Crime Cells and the I4C

The frontline defense against digital criminality is executed by the specialized Cyber Crime Cells of State Police forces. The operational effectiveness of these units has grown exponentially. For instance, the Cyber Fraud Mitigation Centre (CFMC) established by the Uttar Pradesh Police exemplifies state-level operational success. Leveraging a dedicated, high-capacity call center and immediate, real-time coordination with banking institutions, the UP Police achieved the nation's third-highest lien percentage in 2024. They successfully froze over ₹484 crore in defrauded funds within the critical "golden hour" of the crime, preventing transnational syndicates from siphoning the money out of the domestic banking system.[16]

There is an urgent, undeniable need for the widespread establishment of designated Special Cyber Courts staffed exclusively by judicial officers trained extensively in cyber law and digital forensics. While states like Uttar Pradesh are proactively establishing dedicated cyber police stations in 57 districts to investigate crimes, the parallel establishment of designated Cyber Sessions Courts to try these cases is progressing highly unevenly across the country. State Judicial Academies such as the

[15] The Digital Personal Data Protection Act, 2023 (Act 22 of 2023), s. 17
[16] UP tops nation in cyber fraud recovery", The Times of India (2025)

Judicial Training & Research Institute (JTRI) in UP are aggressively conducting capacity-building programs, training judicial officers in appreciating electronic evidence and understanding algorithmic jurisdictions. However, without structurally ring-fencing complex digital cases into technical fast-track courts, the principle of the "speedy trial" enshrined in the BNSS will remain practically unattainable, emboldening cybercriminals who rely on judicial delays to evade conviction.[17]

VII. CONCLUSION

India's legal framework for regulating cybercrimes has undergone a profound, historic metamorphosis, definitively transitioning from a state of post-facto legislative patching to an era of deliberate, technology-integrated penal reform. The constitutional foundation remains highly robust; the Supreme Court has meticulously engineered a dynamic jurisprudential equilibrium wherein the fundamental rights to digital free speech, informational privacy, and algorithmic equality serve as non-negotiable constitutional counterweights to the state's urgent imperative to secure cyberspace against digital terrorism, financial syndicates, and targeted harassment.

The introduction of the new criminal Sanhitas the BNS, BNSS, and BSA signals a remarkable legislative maturation. By statutorily recognizing organized cyber syndicates, elevating electronic records to the pedestal of primary evidence, creating specific offenses for digital gender violence, and embedding digital procedures into the absolute core of criminal investigations, India has largely eradicated the analog ambiguities that previously plagued digital prosecutions. The substantive law is now largely aligned with the technical reality of the 21st century.

However, statutory excellence must inevitably be matched by structural and institutional capability. As this analysis demonstrates, critical fault lines and operational vulnerabilities persist. Overlapping jurisdictions between the BNS and the IT Act threaten to create redundant regulatory regimes. The expansive exemptions for law enforcement under the DPDPA raise valid fears of surveillance overreach. Furthermore, the immense friction between law enforcement demands for message traceability and the cryptographic necessity of end-to-end privacy remains an unresolved constitutional dilemma. Most pressingly, the procedural mandates of the

[17] E-Committee Newsletter, Supreme Court of India (Sept. 2025)

BNSS and BSA highlight an acute, systemic infrastructure deficit in state forensic laboratories and judicial tribunals. For India to fully operationalize this formidable, modernized legal framework and sustain its trajectory as a secure, Tier-1 digital economy, future policy vectors must fiercely prioritize massive financial investments in forensic infrastructure, the nationwide establishment of Special Cyber Courts, and the continuous, rigorous harmonization of penal statutes with the uncompromising mandates of fundamental constitutional rights.