Volume 3, Issue 3 ISSN 2582-743X

The Intersection of Technology and Law: Evaluating the Efficacy of Indian Legislative Frameworks in Combating Cyber Crime

Mr. Tanmay Dubey
Assistant Professor
Mansarovar Global University,
Sehore, Madhya Pradesh

ABSTRACT

The increasing integration of digital technologies into India's economic and social framework has catalyzed the rise of cybercrimes that threaten individual rights, financial integrity, and national security. While India's legislative instruments such as the Information Technology Act, 2000 and Bhartiya Nyaya Sanhita, 2023 attempt to regulate cyberspace, their efficacy remains limited in light of technological advancement, jurisdictional limitations, weak enforcement, and lack of legal clarity. This paper critically evaluates the evolution and effectiveness of the Indian legal framework for cybercrime regulation by examining statutes, judicial precedents, enforcement mechanisms, and comparative international approaches. The objective is to offer a doctrinal and empirical assessment of how Indian law can better address cyber threats while balancing civil liberties and digital innovation.

Keywords*:* Cyber Crime, Information Technology Act, Digital Evidence, Data Privacy, Enforcement, Jurisdiction, Legal Reform, Cybersecurity, Technology Law

INTRODUCTION

The interface between law and technology represents a dynamic and often volatile relationship in modern legal systems. In India, this relationship is increasingly tested by the exponential growth of digital technologies. With more than 850 million internet users and the proliferation of fintech, e-governance, social media, and digital healthcare platforms, India has become a digital economy at scale.[1] However, this digital surge is accompanied by a dramatic increase in cyber crimes, ranging from financial frauds and data theft to online harassment, misinformation, and cyberterrorism.

The structural features of cyberspace, its anonymity, border-lessness, and decentralization, make cyber-crimes difficult to trace and prosecute. This necessitates a robust, adaptive legal framework that can respond effectively to digital threats. The legal response in India is principally centered around the Information Technology Act, 2000 and its 2008's amendment, which attempted to

[1] *850 mn internet users key to India's $1 trillion digital economy: Report*, The Economic Times (May 16, 2018), https://m.economictimes.com/tech/ites/850-mn-internet-users-key-to-indias-1-trillion-digital-economy-report/articleshow/64193359.cms.

Volume 3, Issue 3 ISSN 2582-743X

expand the scope of punishable cyber offences. Supplementing this are provisions from the Bharatiya Nyaya Sanhita, 2023 and rules under the BNSS. Yet, serious gaps remain in terms of enforceability, technical capacity of law enforcement agencies, coordination with international authorities, and the protection of digital privacy and civil liberties.

The rapid digitization of governance, commerce, healthcare, education, and financial services has transformed India into a predominantly digital society. Initiatives like Digital India, JAM trinity (Jan Dhan-Aadhaar-Mobile), and the Unified Payments Interface (UPI) have expanded access to technology but have also simultaneously created vulnerabilities in cyberspace. The democratization of internet access has enabled new forms of communication and economic activity, but it has also exposed millions to identity theft, digital fraud, misinformation, and various forms of online harassment. These evolving cyber threats demand a proportional and calibrated legal response.

Cyber-crime is not merely a technical disruption, it is a complex socio-legal issue that affects fundamental rights, national security, and democratic integrity. With the internet acting as a vehicle for both freedom of expression and criminal behavior, lawmakers are challenged to strike a careful balance between enabling digital innovation and ensuring lawful regulation. The multifaceted nature of cyber offences, their cross-border implications, and the rapid development of new technologies require Indian law to be responsive, flexible, and forward-looking.

This paper critically evaluates whether the Indian legal system, as it stands today, adequately addresses the scale and sophistication of contemporary cyber-crimes. It delves into the strengths and weaknesses of the legal framework, assesses the role of judicial intervention, examines implementation challenges, and explores comparative approaches from other jurisdictions. In doing so, it highlights the urgent need for a comprehensive, inclusive, and technologically adaptive legal regime that safeguards both digital freedoms and public safety.

DEFINING CYBER CRIME IN THE INDIAN LEGAL CONTEXT

Cyber-crime in India lacks a uniform definition. The Information Technology Act, 2000 does not define “cyber-crime” per se but creates offences involving computers, digital systems, and networks. Broadly, cyber-crime refers to any illegal act committed using a computer or network, or directed against such infrastructure. These include unauthorized access, data theft, identity fraud, online defamation, cyber pornography, stalking, and cyber terrorism.

The rise in cyber-crimes is empirically verifiable. According to the National Crime Records Bureau (NCRB), cyber-crime cases rose from 27,248 in 2018 to over 65,000 in 2022, marking a 140% increase in four years. A significant proportion of these crimes involve financial fraud,

Volume 3, Issue 3 ISSN 2582-743X

phishing, and impersonation, targeting vulnerable populations unfamiliar with cybersecurity practices.[2]

The diversity of cyber-crimes has also grown, with new-age crimes like ransomware attacks, cryptocurrency-related fraud, AI-driven identity spoofing, and synthetic pornography challenging traditional enforcement models. As India moves toward greater digitization through initiatives like Digital India, BharatNet, and Aadhaar-linked services, the risk landscape grows even broader.

STATUTORY FRAMEWORK: THE INFORMATION TECHNOLOGY ACT, 2000

The Information Technology Act, 2000 was enacted to provide legal recognition for electronic commerce and digital signatures. Its primary objectives were commercial, not criminal. However, with the IT (Amendment) Act, 2008, significant cyber-crimes were criminalized through the inclusion of Sections 66 to 74.

Section 66 penalizes hacking, while Section 66C criminalizes identity theft involving passwords or unique identification features. Section 66D deals with cheating by personation using computer resources. Section 66E punishes violation of privacy by capturing images without consent. Section 66F addresses cyber terrorism, a broad provision that can be invoked against any activity threatening the sovereignty or integrity of India through digital means. These provisions impose penalties ranging from imprisonment to fines, depending on the gravity of the offence.

Obscene or sexually explicit content in digital form is dealt with under Section 67 and 67A, with more stringent provisions under Section 67B for child pornography. However, terms such as “obscenity” remain undefined, inviting discretionary application and potential misuse.

Despite these legislative efforts, the Act has been criticized for definitional vagueness, disproportionate punishments, and overlapping jurisdiction with the Bharatiya Nyaya Sanhita, 2023. The now-struck-down Section 66A of the Act, which penalized sending "offensive" messages via electronic communication, was held unconstitutional in *Shreya Singhal v. Union of India*,[3] for violating Article 19(1)(a) of the Constitution. The Supreme Court found the language of the section vague and overbroad, chilling free speech and allowing arbitrary enforcement.

Additionally, enforcement of the IT Act is hindered by the absence of dedicated cyber benches in courts and insufficient awareness among police officers. Although some states have established cyber cells, their technological and forensic capabilities are inadequate. In most cases, prosecution

[2] Press Information Bureau, *Ministry of Electronics & IT to organize Digital India Dialogues with key stakeholders to accelerate Digital India Programme,* Press Info. Bureau (June 10, 2024), https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2003505.
[3] (2015) 5 S.C.C. 1.

Volume 3, Issue 3 ISSN 2582-743X

rates remain dismally low, pointing to a systemic failure in converting legal mandates into effective deterrents.[4]

SUPPLEMENTING FRAMEWORKS - PROCEDURAL LAWS

Since the IT Act does not cover all dimensions of criminal behavior online, especially when it comes to defamation, threats, obscenity, and physical harm resulting from digital acts, prosecutors routinely rely on provisions of the Bharatiya Nyaya Sanhita, 2023.

Section 316 of the BNS (cheating and dishonestly inducing delivery of property) is commonly invoked in cyber frauds, while Section 73 is used to prosecute cyberstalking. Sections 354 and 356 address criminal defamation, and Section 77 protects against insults to the modesty of women, useful in addressing online harassment.[5]

Crucially, criminal procedure under the Bharatiya Nagarik Suraksha Sanhita, 2023 also applies to cyber-crimes, including investigation, arrest, bail, and trial. However, Section 78 of the IT Act gives police officers of the rank of Inspector and above the power to investigate cyber offences, creating procedural barriers in rural and semi-urban areas where such officers are scarce.[6]

CHALLENGES IN ENFORCEMENT AND INSTITUTIONAL GAPS

A primary obstacle in combating cyber-crime in India lies in enforcement. Many state police departments lack the infrastructure, training, and manpower to tackle sophisticated digital crimes. Forensic labs are overburdened, leading to delays in the retrieval and authentication of electronic evidence, which is crucial under both the IT Act and the BSA. The problem is exacerbated by poor coordination between central and state enforcement agencies, and the transnational nature of many cyber-crimes, which involve servers and perpetrators located outside India.

As of 2024, only a handful of cyber labs, such as the ones established under the Indian Cyber Crime Coordination Centre (I4C), have access to advanced decryption and cyber forensic tools. Even fewer have the capacity to tackle dark web operations or cryptocurrency-related crimes.

JUDICIAL INTERPRETATION AND ROLE OF THE INDIAN JUDICIARY

The Indian judiciary has played a critical role in interpreting cyber law, striking a balance between state interests and individual rights. Through constitutional scrutiny and statutory interpretation, courts have shaped the contours of cyber jurisprudence in India, often compensating for legislative ambiguity or executive inaction.

[4] Information Technology Act, No. 21 of 2000, § 66, India Code (2000).
[5] Bharatiya Nyaya Sanhita, No. 45 of 2023, §§ 73, 77, 316, 354–356, India Code (2023).
[6] Bharatiya Nagarik Suraksha Sanhita, No. 46 of 2023, § 200, India Code (2023).

Volume 3, Issue 3 ISSN 2582-743X

A landmark development occurred in *Shreya Singhal v. Union of India*,[7] where the Supreme Court declared Section 66A of the Information Technology Act, 2000 as unconstitutional. The Court observed that vague terms like "grossly offensive" and "menacing character" violated Article 19(1)(a) of the Constitution and failed the test of reasonable restrictions under Article 19(2). The judgment reinforced the principle that cyberspace cannot be used as a justification to curtail civil liberties without constitutionally valid reasons.

In *K.S. Puttaswamy v. Union of India*,[8] the Supreme Court recognized the right to privacy as a fundamental right under Article 21. Although not a cyber-crime case per se, the judgment has profound implications for data security, surveillance, and profiling in digital spaces. It sets the normative foundation for future legislation dealing with data breaches, unlawful tracking, and AI-driven exploitation.

More recently, in *Ajit Mohan v. Legislative Assembly of Delhi*,[9] the Court discussed the responsibility of social media platforms and the necessity of parliamentary oversight in the digital domain. Although the case concerned Facebook's alleged role in inciting communal tensions, it shed light on intermediary accountability, the power of algorithms, and the thin boundary between content hosting and content curation.

Despite these interventions, Indian jurisprudence on cyber-crime remains nascent and often reactive. Courts have not yet developed a consistent jurisprudence on cyber forensics, attribution of online conduct, or degrees of platform liability. Additionally, bail jurisprudence in cyber offences remains inconsistent, with courts relying on general criminal law principles rather than laying down technology-specific standards for mens rea or evidentiary sufficiency.

EMERGING THREATS AND NEW-GENERATION CYBER CRIMES

India's legal regime is further challenged by the emergence of next-generation cyber threats that were not foreseen when the IT Act was drafted. These include deepfakes, crypto crimes, cyber-espionage, biometric data theft, and coordinated disinformation campaigns using artificial intelligence.

Deepfake technology, which uses AI to manipulate images and videos, has already been used to defame political figures and celebrities, raising concerns about consent, identity theft, and harassment. While Sections 66C and 66E of the IT Act, 2000 can be invoked, they are insufficiently nuanced to address synthetic content created using machine learning techniques.

[7] (2015) 5 S.C.C. 1 (India).
[8] (2017) 10 S.C.C. 1 (India).
[9] (2021) 5 S.C.C. 1.

Volume 3, Issue 3 ISSN 2582-743X

Cryptocurrency-related crimes present another unregulated area. India lacks a comprehensive legislative framework to investigate or prosecute crimes involving digital assets like Bitcoin or Ethereum. The Reserve Bank of India had imposed a banking ban on cryptocurrencies in 2018, which was struck down in *Internet and Mobile Association of India v. Reserve Bank of India*,[10] on the grounds that the ban disproportionately restricted the right to carry on trade.

The growth of surveillance technologies by both state and private actors also raises legal questions. The Pegasus spyware controversy revealed vulnerabilities in the legal regime governing lawful interception, which is currently governed by Sections 69 and 69B of the IT Act and Rule 419A of the Indian Telegraph Rules, 1951. These provisions lack transparency and judicial oversight, making them susceptible to abuse.

Moreover, cyber-attacks targeting critical infrastructure such as power grids, hospitals, and financial institutions are increasingly being reported. These offences, potentially falling under the ambit of cyber terrorism under Section 66F of the IT Act, 2000 raise urgent questions of national security, state preparedness, and international cooperation.

COMPARATIVE LEGAL APPROACHES: LESSONS FROM THE EU AND US

India's cyber-crime regulatory approach can benefit from a comparative analysis of other jurisdictions, particularly the European Union and the United States, both of which have adopted technologically adaptive legal standards.

The European Union has developed a comprehensive data protection and cyber security architecture. The General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, imposes strict obligations on data controllers and processors and mandates notification of personal data breaches within 72 hours. It also recognizes a right to be forgotten and provides for significant monetary penalties, making it one of the most rigorous frameworks globally.[11]

Additionally, the EU Cybersecurity Act, Regulation (EU) 2019/881, strengthens the role of ENISA (European Union Agency for Cybersecurity) and introduces a cybersecurity certification framework for ICT products and services.

In contrast, the United States follows a sector-specific approach, with laws like the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, and the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2510–2523. The U.S. Department of Justice has prosecuted cyber espionage and financial fraud under these statutes, including high-profile indictments against foreign hackers.

[10] (2020) 10 S.C.C. 274 (India).
[11] Regulation (EU) 2016/679 of the European Parliament and of the Council, 2016 O.J. (L 119) 1 (General Data Protection Regulation).

Volume 3, Issue 3 ISSN 2582-743X

India's centralized model, primarily reliant on the IT Act, lacks such institutional diversity and flexibility. Moreover, India has not yet acceded to the Budapest Convention on Cybercrime, the only international treaty on cyber-crime, largely due to concerns about data sovereignty. Accession could, however, enhance India's cooperation in cross-border investigations and improve its access to digital evidence stored overseas.[12]

INSTITUTIONAL SHORTCOMINGS AND ENFORCEMENT DEFICITS

Beyond statutory deficiencies, India's cyber-crime framework suffers from deep institutional deficits. Although the Indian Cyber Crime Coordination Centre (I4C) was established by the Ministry of Home Affairs to provide a national response mechanism, its operationalization has been uneven across states. Only a few metropolitan cities like Hyderabad, Bengaluru, and Mumbai have fully functional cyber-crime police stations equipped with forensic labs.

Most police officers are inadequately trained in cyber investigation protocols, digital evidence handling, or coordination with Computer Emergency Response Teams (CERT-IN). This results in delayed investigations, wrongful arrests, or failure to preserve volatile digital evidence that is easily altered or deleted. The rules of evidence under the BSA, particularly Sections 61, require certification for electronic evidence, but courts and prosecutors often fail to comply with these procedural mandates, leading to acquittals or case dismissals.

The CERT-In Guidelines, 2022, which mandate the reporting of certain types of cyber incidents within six hours, represent a step forward. However, the penalties for non-compliance are minimal, and the absence of a Data Protection Authority under the Digital Personal Data Protection Act, 2023 has left a vacuum in coordinated enforcement.[13]

POLICY GAPS AND THE NEED FOR LEGISLATIVE REFORM

The current Indian cyber-crime framework, although expansive in some areas, is fragmented and outdated in others. Technology has evolved faster than the legislative response, leading to regulatory lag and under-enforcement. Several policy gaps persist, particularly in relation to data protection, AI-generated threats, cross-border cooperation, and the liability of intermediaries.

One major concern is the lack of a unified cyber-crime statute. While the Information Technology Act addresses digital offences and the Bharatiya Nyaya Sanhita, 2023 supplements traditional crimes committed via digital means, the absence of a consolidated code creates interpretive

[12] Council of Europe, Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185.
[13] CERT-In, Guidelines for Cyber Security Incident Reporting, Ministry of Electronics and Information Technology, Apr. 28, 2022.

Volume 3, Issue 3 ISSN 2582-743X

challenges. Scholars have noted that Indian cyber law lacks the "structural integration" needed to respond to complex multi-jurisdictional offences.[14]

The Digital Personal Data Protection Act, 2023, although an important development, focuses primarily on data fiduciaries and consent-based processing. It does not clearly define government surveillance powers, nor does it offer safeguards for data collected during criminal investigations. As a result, even when data is collected in the course of prosecuting cyber-crimes, questions about its admissibility and legality remain.[15]

Furthermore, India has yet to adopt a separate legal framework for critical information infrastructure protection. In the absence of detailed laws like the U.S. Cybersecurity Information Sharing Act or the EU's NIS2 Directive, India continues to rely on executive notifications under Section 70 of the IT Act, which lack accountability mechanisms.[16]

INTERMEDIARY LIABILITY AND SAFE HARBOUR PROVISIONS

One of the most contested areas in Indian cyber law is the liability of intermediaries, such as social media platforms and content-sharing websites. Section 79 of the Information Technology Act, 2000 grants a "safe harbour" to intermediaries from liability for third-party content, provided they observe due diligence and take down unlawful content when notified.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended in 2023, introduced stricter obligations on intermediaries, including appointment of grievance redressal officers, 24-hour takedown compliance, and traceability of originators of unlawful messages. However, these Rules have been challenged for potentially violating privacy and freedom of expression under Articles 19 and 21 of the Constitution. Critics argue that such traceability mandates could result in the weakening of end-to-end encryption and chilling effects on speech.[17]

Moreover, the IT Rules fail to differentiate between different categories of intermediaries. Unlike the EU's Digital Services Act, which classifies platforms based on user base and systemic risk, Indian law applies a largely uniform approach. This raises compliance burdens for smaller startups while doing little to enhance accountability among major tech firms.

PROTECTING VICTIMS AND STRENGTHENING DIGITAL LITERACY

A critical shortcoming of the Indian cyber-crime framework lies in its treatment of victims. The current law is heavily focused on criminalization and enforcement, with little regard for victim

[14] Rahul Sharma, *Cyber Law: A Comprehensive Study in the Indian Context*, 14 NUJS L. Rev. 201, 202 (2021).
[15] Digital Personal Data Protection Act, No. 22 of 2023, India Code (2023).
[16] *Supra* note 12.
[17] Apar Gupta, *Traceability and the IT Rules: Constitutional Fault Lines*, 38 Nat'l L. Sch. India Rev. 45 (2022).

Volume 3, Issue 3 ISSN 2582-743X

support, restitution, or rehabilitation. Unlike sexual or domestic violence victims, cyber-crime victims receive minimal psychosocial or legal support. This leads to underreporting, particularly in cases involving online harassment, sextortion, or LGBTQ+ targeted hate crimes.

Victims of financial fraud, especially the elderly and rural users, are often left without remedies due to procedural delays and lack of digital evidence admissibility. While the National Cyber Crime Reporting Portal was launched to ease access to reporting, delays in investigation, jurisdictional confusion, and lack of follow-up continue to undermine its utility.

Research suggests that digital literacy plays a critical role in preventing cyber victimization. A study by P. Raghavan and S. Lal in *Digital Vulnerabilities and Cyber Awareness in India's Tier-2 Cities*, found that over 70% of respondents lacked knowledge of secure browsing practices, multi-factor authentication, or phishing prevention, making them soft targets for cyber criminals.[18]

NATIONAL SECURITY, SURVEILLANCE, AND THE CONSTITUTIONAL BALANCE

Cyber-crime regulation increasingly intersects with matters of national security and state surveillance. The Indian government has justified expanding digital monitoring tools under the guise of counter-terrorism and information warfare. However, without a formal legal framework or independent oversight, such surveillance risks violating fundamental rights.

Sections 69 and 69B of the Information Technology Act, 2000 empower the government to intercept, monitor, and decrypt any information "in the interest of sovereignty and integrity of India." These provisions lack safeguards such as prior judicial approval, time-bound limitations, or transparency reports, making them vulnerable to misuse.

In *K.S. Puttaswamy*, the Supreme Court held that any restriction on privacy must satisfy the triple test of legality, necessity, and proportionality. Yet, India has not enacted a Surveillance Regulation Act akin to the UK's Investigatory Powers Act or the U.S. Foreign Intelligence Surveillance Act. Scholars such as N. Allahrakha argues that "India's digital surveillance regime is constitutionally deficient due to executive discretion unchecked by judicial accountability.[19]

GENDERED DIMENSIONS OF CYBER CRIME

Cyber-crimes disproportionately affect women and gender minorities. Online abuse, doxing, deepfake pornography, stalking, and threats of violence are used to silence or intimidate them. According to a UN Women report on digital violence in South Asia, 41% of Indian women who

[18] P. Raghavan & S. Lal, *Digital Vulnerabilities and Cyber Awareness in India's Tier-2 Cities*, 19 Indian J.L. & Tech. 187 (2022).
[19] N. Allahrakha, *Constitutional Safeguards for Digital Rights and Privacy*, 34 NALSAR L. Rev. 119, 130 (2024).

Volume 3, Issue 3 ISSN 2582-743X

experienced online abuse reported mental health impacts, but only 12% sought legal recourse due to victim-blaming and procedural apathy.

Indian law does not offer gender-sensitive remedies beyond general provisions of the IPC or IT Act. While initiatives like the Cyber Crime Volunteers Program seek to address content monitoring, their lack of transparency raises concerns of vigilantism. There is an urgent need to establish specialized units for gender-based cyber violence, train law enforcement in trauma-sensitive approaches, and offer institutional support including legal aid and digital safety tools.

Academic literature also points out that the structural design of digital platforms perpetuates gender bias. S. Roy's study, *Digital Gender Violence and Legal Responses in India*,[20] recommends gender audits for online content moderation algorithms and inclusion of feminist jurisprudence in cyber-crime adjudication.

CONCLUSION & THE WAY FORWARD

India stands at a critical juncture in its cyber law evolution. With digital technologies rapidly transforming the way individuals, institutions, and governments function, the legal framework must respond with equal agility and foresight. The country has made notable strides through its enactment of the Information Technology Act, 2000 procedural reforms, and recent efforts like the Digital Personal Data Protection Act, 2023. However, the speed, sophistication, and scale of cyber threats today far outstrip the capabilities of existing legal and institutional frameworks.

The dual burden of increasing cyber-crime and inadequate legal infrastructure creates an ecosystem where victims often remain unprotected, law enforcement remains under-trained, and legal remedies remain inaccessible. While courts have occasionally intervened to check state overreach or clarify constitutional boundaries in digital spaces, there remains a notable absence of proactive jurisprudence and specialized adjudication mechanisms. Furthermore, the fragmented approach of relying on multiple statutes without a harmonized cyber-crime code leads to inconsistencies in prosecution and confusion during enforcement.

The reactive nature of Indian cyber policy often means that regulation follows harm. Rather than anticipating emerging technological risks such as AI-generated content, quantum decryption, or blockchain anonymity, the law tends to respond only after large-scale damage has occurred. This leaves users vulnerable and places significant pressure on the state to investigate crimes after the fact rather than preventing them. The importance of a forward-looking, anticipatory cyber law framework cannot be overstated.

Equally important is the role of education, training, and literacy in addressing the cyber-crime problem. Legal instruments, no matter how well-crafted, cannot succeed in isolation. A digitally

[20] S. Roy, *Digital Gender Violence and Legal Responses in India*, 22 J. Indian Soc'y Criminal. 67 (2023).

Volume 3, Issue 3 ISSN 2582-743X

literate population, supported by trained law enforcement officers and a tech-aware judiciary, is essential for any law to succeed in cyberspace. The absence of robust training programs, especially in Tier 2 and Tier 3 regions, means that a large part of India remains unequipped to navigate cyber threats, let alone seek redressal through formal legal channels.

Policy design must also focus on inclusivity and equity. Cyber-crime disproportionately impacts vulnerable groups such as women, children, the elderly, and LGBTQ+ individuals. The legal system must recognize this differentiated impact and ensure that its tools of protection are both accessible and sensitive to the specific harms faced by these groups. A one-size-fits-all approach will only reinforce the structural gaps in access to justice.

India must also improve its capacity for international cooperation. Cyber-crime is inherently transnational, and many offences involve actors or data located outside Indian jurisdiction. Mutual legal assistance treaties, extradition processes, and real-time information sharing frameworks need to be modernized and digitized. Building trusted relationships with global platforms and foreign law enforcement agencies is essential for any meaningful cross-border enforcement.

A reimagination of cyber policing is also overdue. Dedicated cyber-crime units should be established in every district, equipped not only with technological tools but also with cyber forensic labs and legal advisors. Their independence from political interference, budgetary support, and connection to centralized monitoring systems would dramatically improve investigative outcomes and build public confidence in digital law enforcement.

Any effort to strengthen cyber law must be grounded in constitutional principles. As India regulates cyberspace, it must balance national security with individual freedoms, efficiency with accountability, and innovation with safety. A rights-respecting approach to cyber governance, rooted in transparency, accountability, and due process, will ensure that India does not just regulate the digital world, but leads it with vision and responsibility.