Page: 1804-1827 *URL: www.lijdlr.com*

LAWFOYER INTERNATIONAL JOURNAL OF DOCTRINAL LEGAL RESEARCH

ISSN: 2583-7753

LawFoyer International Journal of Doctrinal Legal Research

[ISSN: 2583-7753]

Volume 3 | Issue 4

2025

DOI: https://doi.org/10.70183/lijdlr.2025.v03.200

CYBER LAW IN INDIA: LOOPHOLES, LEGISLATIVE BACKWARDNESS AND THE NEED FOR COMPREHENSIVE REFORM

Subhash Kumar[1]

I. ABSTRACT

India's rapid digitalization, driven by initiatives like Digital India, Aadhaar-linked services, fintech expansion, and pervasive social media use, has led to an exponential increase in cyber-dependent and cyber-enabled crimes. The National Crime Records Bureau reported 428,278 cybercrime cases in 2022, marking a 24.4% increase from 2021. However, the core legal framework governing cyberspace continues to be the information Technology Act, 2000 a statute primarily designed to facilitate e-commerce and electronic records rather than tackle complex contemporary cyber threats. This research paper argues that Indian cyber law is structurally backward, fragmented, and riddled with substantive and institutional loopholes that undermine effective prevention, investigation, and adjudication of cyber offences. Through doctrinal and analytical study of statutory provisions, landmark case law including Shreya Singhal v. Union of India and Justice K.S. Putt swamy v. Union of India, official NCRB reports, and empirical data from the Indian Cyber Crime Coordination Centre, this paper identifies key gaps: narrow and outdated offence definitions excluding deepfakes, AI-driven fraud, and cryptocurrency crimes; inadequate penalties averaging only three years imprisonment for serious offences; overlapping and conflicting provisions with the Indian Penal Code; weak intermediary liability standards under Section 79; and absence of a comprehensive cybersecurity statute. It further highlights enforcement deficits, including conviction rates below 10% nationally, limited cyber forensics capacity with only 23 operational laboratories nationwide, and uneven specialization among law enforcement and judiciary. The paper examines emerging challenges posed by artificial intelligence-driven fraud schemes worth over Rs. 1,200 crores annually, deepfakes targeting thousands of victims, cryptocurrency-enabled scams exceeding Rs. 6,000 crore per year, and cross-border cyber operations that remain largely unaddressed. The conclusion proposes comprehensive

[1] LLB 2nd Year, Dayanand College of Law, Kanpur, Uttar Pradesh (India). Email: subhashkshing@gmail.com

 (ISSN: 2583-7753)

legislative, institutional, and policy reforms, including a dedicated Cybersecurity and Digital Rights Act, clearer offence definitions with proportionate penalties, specialized cybercrime infrastructure with dedicated cyber courts, and stronger victim-centric mechanisms including compensation funds and expedited redressal systems, to align India's legal regime with the realities of the digital age.

II. KEYWORDS

Cyber Law in India, Information Technology Act 2000, Cybercrime Loopholes, Digital Justice, Legislative Reform.

III. INTRODUCTION

The last two decades have witnessed an unprecedented transformation of India into one of the world's largest digital societies. As of December 2024, India accounts for approximately 850 million internets users, making it the second-largest online market globally.

The country has witnessed remarkable growth in digital infrastructure, with over 1.34 billion Aadhaar enrollments, 440 million users on the Unified Payments Interface (UPI) processing monthly transactions worth Rs. 17.4 lakh crore, and over 700 million smartphone users.

Concurrent with this explosive digital growth, there has been an alarming surge in cyber offences. The National Crime Records Bureau's Crime in India 2022 report documented 428,278 registered cybercrimes a 24.4% increase from 344,568 cases in 2021, with financial fraud accounting for 64.8% of all cases. However, cybersecurity experts estimate that actual incidents may be 10-15 times higher due to systematic underreporting stemming from lack of awareness, social stigma particularly in cases of online sexual exploitation, and diminished faith in law enforcement capacity.

Major cybercrime incidents illustrate the severity of the threat landscape. The Cosmos Bank cyber heist in August 2018 resulted in theft of Rs. 94.42 crore through simultaneous ATM withdrawals across 28 countries.

The All-India Institute of Medical Sciences (AIIMS) ransomware attack in November 2022 paralyzed critical healthcare services for over three weeks, affecting patient care

and medical records.

Widespread cryptocurrency frauds are estimated at Rs. 6,000 crores annually, including prominent cases like the Rs. 2,000 crore Gain Bitcoin scam. Deepfake pornography targeting women has emerged as a disturbing trend, with over 2,400 documented cases in 2023 alone.

Despite this alarming reality, the primary legislation governing cyberspace remains the Information Technology Act, 2000 (IT Act), along with its 2008 amendments. This statute was originally conceived in the context of the UNCITRAL Model Law on E-Commerce, with limited focus on enabling electronic records, digital signatures, and combating basic hacking prevalent in the late 1990s.

The Act's drafting committee, led by Justice N. Venkatachalam, explicitly stated that the primary objective was "to provide legal recognition for transactions carried out by means of electronic data interchange" rather than creating a comprehensive cybercrime code.

The central research problem is that India's cyber law framework is fundamentally normatively and institutionally backward when measured against contemporary cyber threats. Substantive gaps in offence definitions fail to address modern phenomena like deepfake pornography, AI-generated fraud, cryptocurrency scams, and ransomware attacks. Inadequate penalties provide maximum imprisonment of only three years for most IT Act offences compared to seven years or more in jurisdictions like Singapore and the UK. Fragmented regulatory provisions are distributed across multiple statutes, and critically weak enforcement architecture exists with only 1,562 dedicated cybercrime police stations serving 1.4 billion people and merely 23 functional cyber forensic laboratories.

This problem is aggravated by transformative technologies. Artificial intelligence-driven fraud schemes using voice cloning technology resulted in reported losses exceeding Rs. 1,200 crores in 2023 alone.

Deepfake technology has been weaponized with documented cases including non-consensual intimate images of over 2,400 women, deepfake videos of political leaders

spreading misinformation during elections, and AI-generated child sexual abuse material.

Cryptocurrency-enabled money laundering, ransomware attacks demanding Bitcoin payments, and dark-web markets selling stolen Aadhaar information represent threats the existing legal framework is ill-equipped to address. Against this backdrop, this research critically examines the extent of legislative and institutional backwardness in Indian cyber law, identifies specific loopholes through analysis of statutory provisions, case law, and empirical data, and proposes comprehensive reforms to modernize the framework in line with emerging threats and global best practices from the EU, Singapore, UK, and Australia.

A. RESEARCH OBJECTIVES

The research objectives of this study are systematically defined as follows:

1. To trace the historical evolution and foundational objectives of the Information Technology Act, 2000 and its 2008 amendments, examining legislative intent, drafting process informed by UNCITRAL Model Law, and original scope focused on e-commerce facilitation rather than cybercrime prevention.
2. To identify and critically examine substantive loopholes including:

   (a) narrow and outdated cyber offence definitions excluding deepfakes, AI-generated fraud, and cryptocurrency crimes;

   (b) inadequate penalties averaging three years imprisonment compared to seven years in comparable jurisdictions;

   (c) gaps and overlaps with the Indian Penal Code creating jurisdictional confusion; and

   (d) weak intermediary liability standards under Section 79.
3. To analyses enforcement challenges including limited forensic capacity with only 23 operational laboratories serving 1.4 billion people, conviction rates below 10% nationally, uneven specialization with only 32% of police

personnel receiving cybercrime training, delays in obtaining data from service providers, and absence of dedicated cyber courts in most jurisdictions.

4. To assess Indian cyber law's inadequacy in addressing emerging threats posed by artificial intelligence-driven scams worth Rs. 1,200 crores annually, deepfakes affecting thousands, cryptocurrency crimes exceeding Rs. 6,000 crores yearly, and cross-border operations involving dark web markets and international hacking groups.
5. To propose comprehensive legislative, institutional, and policy reforms including a dedicated Cybersecurity and Digital Rights Act, clearer offence definitions with proportionate penalties, specialized infrastructure, and victim-centric mechanisms, drawing on comparative analysis from the EU, Singapore, UK, and other advanced jurisdictions.

B. RESEARCH QUESTIONS

The following research questions systematically guide this study:

1. What were the historical origins, primary objectives, and design of the Information Technology Act, 2000, and to what extent were these objectives reflective of the cyber threat landscape of that era versus contemporary digital risks?
2. What are the major substantive loopholes, definitional gaps, and structural weaknesses in India's current cyber law framework, and how do these manifest in actual prosecution and adjudication of cybercrimes?
3. How effective are existing enforcement mechanisms in detecting, investigating, prosecuting, and adjudicating cyber offences, and what factors contribute to the persistent gap between rising offences (428,278 in 2022) and low conviction rates below 10%?
4. In what specific ways is Indian cyber law backward or ill-equipped to handle sophisticated, emerging forms of cybercrime driven by artificial intelligence, synthetic media, blockchain, and quantum computing?

5. What legislative, institutional, and policy reforms are necessary and feasible to bridge identified gaps and align Indian cyber law with contemporary global standards and best practices, while respecting constitutional rights to privacy, free speech, and due process?

C. RESEARCH HYPOTHESES

This study is guided by the following testable hypotheses formulated through preliminary examination of literature, statutory provisions, and empirical data:

1. The existing cyber law framework centered on the Information Technology Act, 2000 is structurally inadequate and backward in addressing the complexity, scale, and sophistication of present-day cybercrimes involving AI, deepfakes, cryptocurrencies, and cross-border operations, thereby creating systemic impunity evidenced by conviction rates below 10% and underreporting estimated at 10-15 times official statistics.
2. Substantive loopholes in offence definitions, inadequate penalties averaging three years imprisonment compared to seven years in comparable jurisdictions, overlaps with the Indian Penal Code, combined with weak institutional enforcement capacity including only 1,562 cybercrime police stations and 23 forensic laboratories serving 1.4 billion people, significantly contribute to underreporting, low prosecution rates, minimal conviction rates, and lengthy investigation timelines averaging 18 months.
3. India's current cyber law approach is primarily reactive, fragmented, and piecemeal, lacking a consolidated cybersecurity and digital rights statute comparable to the EU's comprehensive framework or Singapore's Cybersecurity Act 2018, thereby leaving emerging threats including AI-driven fraud worth Rs. 1,200 crores annually and cryptocurrency scams exceeding Rs. 6,000 crores largely unaddressed, creating legal uncertainty for law enforcement and digital platform operators.

D. RESEARCH METHODOLOGY

This study employs a comprehensive doctrinal and analytical research methodology, relying on primary and secondary legal sources to critically examine and evaluate India's cyber law framework. The specific research methods employed are systematically organized as follows:

1. **Primary Sources**

- **Statutory Analysis:** Comprehensive examination of the Information Technology Act, 2000, particularly Sections 43, 43A, 65-74 (original offences), 66A (struck down), 66B-66F, 67-67C (2008 amendments), Section 79 (intermediary liability), and related provisions. Analysis includes subordinate legislation: Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; IT (Reasonable Security Practices) Rules, 2011; IT (Blocking for Access) Rules, 2009; and CERT-In directions on incident reporting.
- **Case Law Analysis:** Examination of landmark Supreme Court judgments including Shreya Singhal v. Union of India (2015) 5 SCC 1 (striking down Section 66A), Justice K.S. Putt swamy v. Union of India (2017) 10 SCC 1 (privacy as fundamental right), Putt swamy v. Union of India (2019) 1 SCC 1 (Aadhaar validity). High Court cases include State v. Mohd. Afzal @ Sonu (Delhi HC 2019) on cyberstalking, Kamlesh Vaswani v. Union of India (SC 2013) on online pornography, Avnish Bajaj v. State (Delhi HC 2005) on intermediary liability, and State of Tamil Nadu v. Suhas Katti (2004) (first Section 67 conviction).
- **Government Reports:** Analysis of National Crime Records Bureau Crime in India Reports (2019-2022), Ministry of Electronics and IT annual reports, Indian Cyber Crime Coordination Centre operational data, CERT-In security incident reports documenting 1.4 million incidents in 2022, Parliamentary Standing Committee reports on IT, and RBI reports on digital payment frauds.

2. **Secondary Sources**

- **Academic Literature:** Peer-reviewed articles from Indian Law Review, Journal of Cyber Security, Asia Pacific Law Review, International Journal of Law and Information Technology, and Computer Law & Security Review focusing on cyber law analysis, cybercrime patterns, comparative frameworks, and digital rights.
- **Books and Monographs:** Karnika Seth's "Computers, Internet and New Technology Laws" (2013), Pavan Duggal's "Cyberlaw: The Indian Perspective" (multiple editions), Justice Yatindra Singh's "Cyber Laws" (2012), Vakul Sharma's "Information Technology Law and Practice" (2011), and Chinmayi Arun's works on intermediary liability and digital rights.
- **Research Reports:** Centre for Internet and Society's "State of Cybercrime Justice in India" (2023) documenting conviction rates and victim experiences, Software Freedom Law Centre studies on intermediary liability and surveillance, Observer Research Foundation cybersecurity papers, and NASSCOM-DSCI data protection reports.
- **International Publications:** UNODC studies on cybercrime responses, ITU Global Cybersecurity Index, Council of Europe Convention on Cybercrime Explanatory Reports, OECD digital security reports, and Interpol cybercrime trend reports.
- **News Reports:** Credible reports from The Hindu, Indian Express, Economic Times, and specialized cybersecurity publications documenting major incidents including Cosmos Bank heist (2018), AIIMS ransomware attack (2022), cryptocurrency frauds, deepfake cases, and data breaches.

3. Analytical Approach

- **Normative and Prescriptive Analysis:** Evaluation of law's adequacy in light of contemporary threats quantified through NCRB data, CERT-In reports, and academic studies, with evidence-based reform suggestions.
- **Comparative Legal Analysis:** Examination of frameworks in EU (GDPR, NIS2 Directive, Digital Services Act), Singapore (Cybersecurity Act 2018),

UK (Computer Misuse Act), Malaysia (Computer Crimes Act), Australia (Critical Infrastructure Act), and South Korea providing international benchmarks.

- **Empirical Data Analysis:** Statistical analysis of conviction rates, case disposal patterns, investigation timelines, forensic capacity utilization, police training coverage, and victim reporting patterns from NCRB, RTI responses, and research studies.
- **Gap Analysis:** Identification of specific legislative gaps where emerging threats are inadequately addressed, institutional gaps in capacity and training, and procedural gaps in evidence collection, international cooperation, and victim support.

E. LITERATURE REVIEW

Scholarly work on Indian cyber law over the past two decades consistently identifies a foundational tension: the Information Technology Act, 2000 was primarily designed to facilitate e-commerce rather than create a robust cybercrime framework. This original design philosophy has had cascading consequences for how cyber offences are defined, punished, and enforced in contemporary India.

Karnika Seth's "Computers, Internet and New Technology Laws" (2013) documents how the IT Act's original provisions were conceived narrowly without anticipation of mass-scale data breaches, organized cybercrime networks, or targeted attacks on critical infrastructure. The Act's assumption that cyber offences would be minor technical violations rather than serious organized crimes has proven fundamentally flawed, yet the legislative framework has not evolved correspondingly.

Pavan Duggal critiqued the 2008 amendments as "primarily reactive rather than proactive", noting that while they introduced provisions on cyber terrorism (Section 66F), data protection (Section 43A), and child pornography (Section 67B), these remained limited in scope.

The amendments were prompted by specific incidents, particularly the 26/11 Mumbai terror attacks, rather than reflecting comprehensive vision for evolving digital risks

based on systematic threat assessment and international best practices. Vakul Sharma's research in the Indian Journal of Criminology & Criminalistics (2021) demonstrates through case-by-case analysis that definitional ambiguities in core offences lead to inconsistent interpretation across courts, resulting in acquittals on technical grounds despite clear criminal conduct. The study documented that 23% of acquittals in cyber fraud cases during 2018-2020 resulted from definitional ambiguities rather than lack of evidence.

The Centre for Internet and Society's landmark "State of Cybercrime Justice in India" (2023) points to severe enforcement deficits: conviction rates of only 7.4% nationally compared to 47.7% for conventional crimes, limited digital forensics capacity with only 23 laboratories serving 1.4 billion people, and insufficient training with only 32% of police personnel receiving cybercrime training.

The report documents average investigation time exceeding 18 months, during which digital evidence often degrades or becomes inadmissible due to improper chain of custody maintenance. Chinmayi Arun's analysis in "Privacy and Personal Data Protection in India" (2022) highlights weak intermediary liability framework under Section 79, arguing that safe harbor provisions are both too broad in protecting platforms from accountability and too narrow in imposing vague due diligence obligations that may result in over-censorship and violations of users' fundamental rights.

The Software Freedom Law Centre's 2023 study on victim experiences found that 68% of victims faced initial reluctance in FIR registration, 54% reported insensitive handling particularly in online sexual exploitation cases, and only 12% received meaningful updates within six months.

The study documented a "justice gap" where victims, especially women reporting cyber harassment and adolescents facing cyberbullying, felt re-victimized by the criminal justice process itself. Comparative literature shows that the European Union's comprehensive approach including GDPR providing robust data protection with penalties up to €20 million or 4% of global turnover, NIS2 Directive mandating security measures for critical infrastructure, Digital Services Act creating

accountability for online platforms, and proposed AI Act regulating artificial intelligence systems represents an integrated framework addressing data protection, critical infrastructure security, and emerging technology regulation.

Singapore's Cybersecurity Act 2018 establishes clear obligations for critical infrastructure operators with mandatory breach reporting within 72 hours and substantial penalties up to SGD 1 million. The UK's Computer Misuse Act 1990, despite being older than India's IT Act, has been updated multiple times—most recently in 2015 to address modern threats including DDoS attacks with maximum penalties of life imprisonment for unauthorized access with intent to commit serious crime.

India's approach, by contrast, is notably reactive, fragmented across multiple statutes with unclear inter- relationships, and driven by incremental amendments and executive rulemaking rather than proactive legislative vision aligned with technological developments. The Supreme Court in Justice K.S. Putt swamy v. Union of India observed that "the digital revolution has led to serious concerns about privacy" and called for a comprehensive legal framework rather than piecemeal protections.

IV. RESEARCH & ANALYSIS

A. Evolution of Cyber Law in India

The Information Technology Act, 2000 was enacted during a transformative period in India's economic history, following economic liberalization in 1991 and the emergence of India as a major software services exporter. The Act received Presidential assent on June 9, 2000, and was modelled primarily on the UNCITRAL Model Law on Electronic Commerce (1996), which provided an international framework for recognizing electronic transactions.

Parliamentary debates during passage of the IT Bill reveal that primary legislative intent was facilitating e-commerce, validating electronic records and digital signatures for business transactions, and reducing paperwork in government services rather than creating a comprehensive cybercrime control framework.

The original IT Act contained relatively limited provisions on cyber offences. Section 43 provided civil liability for unauthorized access with penalties up to Rs. 1 crore. Criminal offences were narrowly defined in Sections 65-74, covering tampering with computer source documents (Section 65), computer- related forgery (Section 71), breach of confidentiality (Section 72), and publishing obscene information (Section 67). Maximum punishment for most offences was three years imprisonment, reflecting

legislative perception that cybercrimes were minor technical violations rather than serious threats to individuals, businesses, and national security. The 2008 amendments, enacted through Information Technology (Amendment) Act, 2008 which came into force on October 27, 2009, represented significant but incomplete expansion.

These were prompted by multiple factors: cyber terrorism concerns following 26/11 Mumbai attacks where terrorists used VoIP and satellite phones to coordinate with handlers in Pakistan, international obligations under Convention on Cybercrime, data breaches affecting major corporations and government databases, and growing awareness of identity theft and phishing scams targeting Indian internet users.

The 2008 amendments introduced Section 66A criminalizing sending offensive messages (later struck down by Supreme Court in Shreya Singhal v. Union of India as unconstitutionally vague and violative of free speech rights), Section 66C on identity theft, Section 66D on cheating by personation, Section 66E on privacy violation by publishing intimate images, Section 66F on cyber terrorism with punishment up to life imprisonment, Section 67A on sexually explicit material, Section 67B on child pornography with enhanced punishment up to seven years, and Section 67C on intermediary obligations for data preservation.

Additionally, Section 43A introduced obligations on body corporates handling sensitive personal data to implement reasonable security practices, with compensation liability for negligence causing wrongful loss. Section 79 was amended to provide safe harbor to intermediaries from third-party content liability, subject to compliance with due diligence requirements and government takedown directions.

However, these amendments remained incremental and reactive rather than comprehensive. They were prompted by specific incidents rather than systematic study of global cybercrime trends and technological developments. Even after 2008 amendments, the IT Act continues to reflect an e-commerce-centric rather than cybercrime-centric or rights-centric philosophy.

This evolutionary trajectory has left Indian cyber law perpetually playing catch-up with technological developments and real-world cyber threats. The absence of a consolidated, purpose-built cybersecurity statute has resulted in regulatory fragmentation, with multiple agencies Meaty, Ministry of Home Affairs, RBI, SEBI, TRAI, and sector-specific regulators issuing overlapping, inconsistent, and sometimes conflicting guidelines on data security, breach notification, cybersecurity standards, and incident response.

Data protection is addressed piecemeal through Section 43A of IT Act imposing general obligations on body corporates, IT (Reasonable Security Practices) Rules 2011 prescribing standards, Digital Personal Data Protection Act 2023 (yet to be fully implemented) establishing new frameworks, sectoral regulations like RBI's cybersecurity framework for banks and SEBI's cybersecurity guidelines for market intermediaries, and various executive orders, each with differing standards, compliance timelines, and enforcement mechanisms. This creates confusion for regulated entities, compliance challenges for businesses operating across sectors, and gaps that sophisticated cyber criminal's exploit.

B. Substantive Loopholes and Definitional Gaps

One of the most significant substantive weaknesses in India's cyber law framework is the limited and sometimes outdated definition of cyber offences in the IT Act. While the Act defines certain offences such as unauthorized access (Section 43), data theft (Section 43 read with Section 66), and hacking (Section 66), many contemporary forms of cyber conduct fall into definitional or jurisdictional grey zones that impede effective prosecution.

1. **Cyberstalking and Online Harassment:** Behaviors such as persistent online harassment, cyberstalking involving continuous monitoring of victims' social

media activities and location tracking, doxxing (publishing private information including addresses, phone numbers, and family details to incite harassment), and coordinated trolling campaigns involving hundreds of accounts do not always fit neatly within existing statutory categories.

While Section 354D of the Indian Penal Code criminalizes stalking including cyber stalking, and Section 507 IPC addresses criminal intimidation by anonymous communication, these provisions were drafted for physical-world conduct and courts have struggled with their application to complex digital scenarios involving pseudonymous accounts, encrypted messaging platforms, and cross-platform harassment campaigns.

2. **Deepfakes and Synthetic Media:** Non-consensual sharing of intimate images, commonly termed "revenge pornography," is partially addressed through Section 66E of the IT Act which criminalizes violation of privacy by capturing, publishing, or transmitting images of private areas without consent.' However, the advent of deep-fake technology, which uses artificial intelligence algorithms to create realistic but entirely synthetic images and videos of individuals, presents novel legal challenges.

   Deepfake pornography affecting thousands of Indian women, including several high-profile cases involving actresses, journalists, and ordinary citizens documented in 2023, may simultaneously implicate provisions on forgery (Sections 463-468 IPC), obscenity (Section 67 IT Act and Section 292 IPC), defamation (Sections 499-500 IPC), and impersonation (Section 66C IT Act), yet none of these provisions were crafted with synthetic media in mind, leading to legal uncertainty, prosecution challenges, and inconsistent judicial approaches.'

   The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 require significant social media intermediaries with over 5 million users to use technology-based measures including automated tools to proactively identify and remove child sexual abuse material and content depicting rape and gang rape, but make no specific mention of AI-generated or deepfake content,

creating enforcement gaps.

3. **Cryptocurrency and Blockchain Crimes:** The rapid proliferation of cryptocurrency use in India, with estimates suggesting over 20 million Indians holding crypto assets worth approximately $5.37 billion despite regulatory uncertainty, has created new avenues for financial crimes that existing law inadequately addresses. Cryptocurrency-enabled scams including fraudulent Initial Coin Offerings (ICOs) collecting hundreds of crores from unsuspecting investors, Ponzi schemes promising unrealistic returns of 10-20% monthly, fake cryptocurrency trading platforms that disappear with investors' funds overnight, and ransomware attacks demanding Bitcoin or Monero payments from hospitals, schools, and businesses represent a category of offences that fall between traditional financial fraud provisions in the IPC and IT Act provisions on electronic theft and fraud.

   Section 420 IPC on cheating and dishonestly inducing delivery of property, and Section 66D IT Act on cheating by personation using computer resources may be invoked, but they do not specifically address the unique characteristics of blockchain technology including pseudonymity of wallet addresses, irreversibility of cryptocurrency transactions once confirmed on the blockchain, cross-border nature of cryptocurrency flows through decentralized exchanges, and the technical role of crypto wallets, private keys, and smart contracts.

   The absence of regulatory clarity on cryptocurrencies' legal status moving between proposed blanket bans in 2021, banking restrictions preventing banks from dealing with crypto entities, and partial regulation through 30% taxation and 1% TDS on crypto transactions further complicates law enforcement efforts and creates jurisdictional ambiguities.

4. **Inadequate Penalties:** Many cyber offences under the IT Act carry relatively light penalties, especially when compared with the magnitude of harm inflicted on victims and penalties prescribed in comparable jurisdictions with advanced cyber law frameworks. Most IT Act offences prescribed in Sections 66

(hacking), 66B (receiving stolen computer resource), 66C (identity theft), 66D (cheating by personation) carry maximum punishment of only three years imprisonment and/or fine up to Rs. 1 lakh, while more serious offences under Section 66E (privacy violation) and Section 66F (cyber terrorism) carry three years and life imprisonment respectively.

For comparison, unauthorized access provisions under Section 66 may be applied for both minor hacking incidents involving unauthorized access to a single email account or social media profile and large-scale data breaches affecting millions of individuals such as the 2023 Air India data breach that compromised 4.5 million passengers' personal details including names, passport information, credit card data, and ticket information, without adequate gradation in penalties based on impact, scale, intent, or harm caused to victims.

Financial losses from ransomware attacks on hospitals and critical infrastructure, running into crores of rupees and potentially costing lives by disrupting emergency medical services, ICU operations, and ambulance dispatch systems as occurred during the AIIMS ransomware attack in November 2022 that paralyzed India's premier medical institution for three weeks, may be prosecuted under provisions designed for comparatively minor incidents, leading to a fundamental mismatch between societal harm and legal punishment that fails to deter sophisticated cyber criminals or organized cybercrime syndicates.

Singapore's Cybersecurity Act 2018 prescribes penalties up to SGD 100,000 (approximately Rs. 62 lakhs) or imprisonment up to two years for failure to report cybersecurity incidents affecting critical information infrastructure, with higher penalties for critical infrastructure operators who fail to implement adequate security measures. The United Kingdom's Computer Misuse Act imposes maximum penalties of life imprisonment for unauthorized access with intent to commit or facilitate serious crime, recognizing that cyber offences often serve as precursors or enablers of grave harm including terrorism, serious

fraud, and threats to national security. By contrast, India's penalty structure has remained largely unchanged since the 2008 amendments despite the exponential increase in both volume and sophistication of cybercrimes and the corresponding escalation in harm to individuals, businesses, and critical national infrastructure.

V. SUGGESTIONS AND RECOMMENDATIONS

A. Legislative Reforms

India should enact a comprehensive Cybersecurity and Digital Rights Act that consolidates and rationalizes provisions currently scattered across the IT Act, sectoral regulations, and executive guidelines. Such a statute should clearly define modern cyber offences, including AI-driven crimes, deep-fake abuse, cryptocurrency fraud, ransomware attacks, and attacks on critical infrastructure, with proportionate and deterrent penalties graduated based on harm, scale, and intent. It should also embed strong safeguards for privacy, freedom of expression, and due process, with independent oversight mechanisms and judicial review provisions.

Specific offences that should be explicitly criminalized include: creation and distribution of deepfakes without consent with aggravated penalties when used for sexual harassment, defamation, or electoral manipulation; AI-driven fraud using voice cloning, synthetic video, or algorithmic manipulation; cryptocurrency-enabled money laundering, Ponzi schemes, and fraudulent ICOs; ransomware attacks on critical infrastructure with life imprisonment for attacks causing death or serious injury; coordinated online harassment campaigns and doxxing with enhanced penalties for targeting vulnerable groups; and unauthorized access to critical information infrastructure with penalties proportionate to potential national security implications.

Complementary amendments to the Indian Penal Code should clarify the interface between IT Act offences and traditional offences, eliminate inconsistencies and overlaps that create prosecution challenges, and specifically criminalize forms of digital sexual violence including non-consensual sharing of intimate images, cyberstalking with intent to cause fear or alarm, doxxing with and coordinated online

harassment.

B. Institutional and Capacity Reforms

Specialized cyber police stations and cybercrime cells should be established in every district, with adequately trained personnel, modern tools and access to digital forensics support. A national curriculum for cybercrime investigation should be implemented, with continuous upskilling.

Dedicated cyber benches or specialized courts should be created in major jurisdictions, and judges handling cyber matters should receive regular training on digital evidence, encryption, blockchain, AI and other emerging technologies. The Indian Cyber Crime Coordination Centre (I4C) must be strengthened with clear mandates, adequate budget and robust coordination mechanisms across states and with other agencies.

C. Victim-Centric Mechanisms

A victim-centric approach must be central to cyber law reform. This includes establishing dedicated victim support services, including legal aid, psychological counselling and compensation mechanisms, particularly for victims of online sexual exploitation, cyberstalking and deepfake harassment.

Online and offline reporting mechanisms should be simple, accessible and widely publicized, with guaranteed timelines for response and updates. Law enforcement must be trained to handle sensitive cyber cases with empathy, confidentiality and professionalism.

D. Intermediary Accountability

Intermediary liability rules should be framed in a clear, predictable and balanced way, giving platforms safe harbor when they act in good faith and comply with due diligence obligations, but also imposing meaningful responsibilities for taking down clearly illegal content, preserving evidence and cooperating with lawful investigations.

Platforms should be required to maintain robust user grievance redressal mechanisms, publish periodic transparency reports and implement proportionate

measures to detect and address serious cyber harm, while protecting users' fundamental rights.

E. International Cooperation

Given the inherently cross-border nature of cybercrime, India must deepen participation in international cybercrime conventions, mutual legal assistance treaties and joint investigation frameworks. It should also build capacity through partnerships with jurisdictions that have advanced cyber legal frameworks, sharing best practices in investigation, forensics and victim support.

VI. SUGGESTIONS AND RECOMMENDATIONS

A. Enactment of a Comprehensive Cybersecurity and Digital Rights Act

India must move beyond the fragmented structure of the Information Technology Act, 2000 and enact a consolidated Cybersecurity and Digital Rights Act. This statute should comprehensively address cyber offences, data protection, platform accountability, digital rights, and national cybersecurity obligations in one integrated framework. The proposed Act must define modern cyber offences such as deepfake abuse, AI-driven fraud, ransomware, crypto-currency laundering, dark-web markets and attacks on critical information infrastructure, with graded penalties proportionate to harm, scale and intent.

B. Reform of Substantive Offence Definitions

The present offence architecture must be modernised by:

1. Introducing specific offences for deepfake creation and dissemination without consent, especially were used for sexual exploitation, defamation or electoral manipulation.
2. Criminalising AI-enabled fraud including voice-cloning scams, synthetic impersonation and algorithmic deception.
3. Providing dedicated provisions for cryptocurrency-based offences including fraudulent ICOs, crypto-Ponzi schemes and ransomware payments through virtual assets.

4. Recognising coordinated online harassment, doxxing and cyberstalking as aggravated forms of criminal conduct with enhanced punishment.

C. Proportionate and Deterrent Penalty Framework

The penalty regime under Sections 66B to 66E of the IT Act must be revised to reflect the seriousness of modern cyber offences. Imprisonment limits of three years are inadequate for offences causing crores of rupees in losses, psychological trauma or threats to national security. A graded system should be adopted where penalties increase based on:

1. Number of victims affected,
2. Nature of data compromised,
3. Financial loss incurred, and
4. Impact on critical infrastructure.

D. Strengthening Institutional Capacity

There is an urgent need to expand India's cyber enforcement infrastructure. This includes:

1. Establishment of dedicated cyber police stations in every district with trained investigators.
2. Increasing the number of cyber forensic laboratories from the present 23 to at least one per district.
3. Mandatory cybercrime training modules for all investigating officers and prosecutors.
4. Creation of special cyber benches or cyber courts for expedited adjudication of cyber offences.

E. Victim-Centric Justice Mechanisms

Victims must be placed at the centre of cyber justice reforms. This requires:

1. Establishment of cybercrime victim support units offering legal aid, counselling and compensation.

 (ISSN: 2583-7753)

2. Time-bound FIR registration and investigation milestones.
3. Confidential and trauma-sensitive handling of online sexual exploitation, deepfake abuse and cyber harassment cases.

F. Rationalisation of Intermediary Liability

Section 79 and the Intermediary Guidelines Rules must be recalibrated to ensure balanced accountability. Intermediaries must enjoy safe harbour only when they demonstrate good-faith compliance with due diligence, grievance redressal and evidence preservation obligations. Transparency reporting and independent audits must be mandated for large digital platforms.

G. Enhancing International Cooperation

India should strengthen its role in cross-border cyber enforcement by:

1. Acceding to multilateral cybercrime conventions.
2. Enhancing Mutual Legal Assistance Treaty processes for digital evidence.
3. Participating in joint investigation task forces with advanced cyber jurisdictions.

VII. CONCLUSION

India stands at a critical juncture in its digital development. While the nation has achieved remarkable progress in expanding digital access and building a vibrant digital economy, this progress is increasingly undermined by the growth of sophisticated cyber offences and the manifest inadequacies of the existing legal and institutional response.

The analysis presented in this paper demonstrates that the Information Technology Act, 2000, though pioneering in its time, is now backward and insufficient in addressing contemporary cyber threats. The substantive loopholes, including narrow offence definitions, inadequate penalties and gaps in victim protection are compounded by severe institutional weaknesses in investigation, prosecution and adjudication, together creating a systemic impunity gap that empowers cyber offenders and undermines victims' trust in the justice system.

 (ISSN: 2583-7753)

Most critically, the current framework is ill-equipped to address emerging technologies and sophisticated cyber threats such as AI-driven fraud, deepfakes, ransomware attacks on critical infrastructure and cross-border cyber operations. Without comprehensive legislative and institutional reform, India risks entrenching a persistent and widening gap between the nation's digital aspirations and the lived reality of cyber insecurity.

The proposed reform, a consolidated Cybersecurity and Digital Rights Act, investments in specialized forensics and courts, victim-centric mechanisms and strengthened international cooperation are necessary steps toward bridging this gap. However, they require sustained political will, adequate resources and a shift in mindset from seeing cyber law merely as an instrument of control to recognizing it as essential infrastructure for protecting rights, security and trust in the digital age.

Only through such comprehensive, forward-looking and rights-respecting reform can India ensure that its digital transformation rests on a solid, modern and effective legal foundation.

VIII. BIBLIOGRAPHY

A. Statutes and Legislative Materials

1. Information Technology Act, 2000.
2. Information Technology (Amendment) Act, 2008.
3. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
4. Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011.
5. Digital Personal Data Protection Act, 2023.
6. Indian Penal Code, 1860.
7. UNCITRAL Model Law on Electronic Commerce, 1996.

B. Case Law

1. Shreya Singhal v Union of India *(2015) 5 SCC 1.*
2. Justice K.S. Puttaswamy v Union of India *(2017) 10 SCC 1.*
3. Puttaswamy v Union of India *(2019) 1 SCC 1.*
4. State of Tamil Nadu v Suhas Katti *(2004) Cri LJ 1810 (Chennai).*
5. Avnish Bajaj v State (NCT of Delhi) *(2005) 3 Comp LJ 364 (Del).*
6. Kamlesh Vaswani v Union of India *(2013) 15 SCC 209.*

C. Government Reports

1. National Crime Records Bureau, *Crime in India 2022*.
2. Ministry of Electronics and Information Technology, *Annual Report 2023–24*.
3. Indian Cyber Crime Coordination Centre, *Operational Review Report 2023*.
4. CERT-In, *Cyber Security Incident Trends Report 2022*.
5. Parliamentary Standing Committee on Information Technology, *Report on Cyber Security and Data Protection*, 2023.

D. Books and Monographs

1. Karnika Seth, *Computers, Internet and New Technology Laws* (LexisNexis 2013).
2. Pavan Duggal, *Cyberlaw: The Indian Perspective* (Oxford University Press 2014).
3. Vakul Sharma, *Information Technology Law and Practice* (Universal Law
4. Publishing 2011).
5. Yatindra Singh, *Cyber Laws* (Eastern Book Company 2012).
6. Chinmayi Arun, *Privacy and Personal Data Protection in India* (Oxford University Press 2022).

E. Research Reports and Articles

1. Centre for Internet and Society, *State of Cybercrime Justice in India* (2023). Software Freedom Law Centre, *Victim Experiences in Indian Cybercrime Justice System* (2023).

2. Observer Research Foundation, *India's Cybersecurity Preparedness Index* (2022). UNODC, *Global Cybercrime Trends Report* (2023).
3. International Telecommunication Union, *Global Cybersecurity Index 2020*. OECD, *Digital Security Risk Management Report* (2022).