Page: 1250-1275 *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 4 | Issue 2

2026

DOI: https://doi.org/10.70183/lijdlr.2026.v04.200

CYBER CRIME AND CHANGING CONTOURS OF CRIMINAL LIABILITY IN CYBERSPACE: A LEGAL AND POLICY PERSPECTIVE

Manasa Ranjan Mishra[1]

I. ABSTRACT

The rampant proliferation and exponential surge of digital technologies have brought about drastic transformation in the genre, and modus operandi of criminal activities in cyberspace. Cyber-crime, being heterogenous unlike conventional crimes, is distinguished by the trait of its obscurity, cosmopolitan presence and technological intricacy that purporting to pose potential threat to traditional nuances of criminal liability embedded in territorial jurisdiction and physical presence. The present paper attempts to trace the genesis of evolving landscape of criminal liability in cyberspace in terms of legal and policy dimensions with special reference to Indian Context. The paper examines the efficacy of prevailing legal frameworks like "IT Act, 2000 and BNS, 2023 in mitigating cyber threats. It tries to unfold strategic issues like ascribing liability in unfamiliar surroundings, jurisdictional disputes in transnational offences, accountability of intermediaries in digital platforms, and evidentiary bottlenecks involved in digital forensics. Further this study emphasizes the burgeoning significance of artificial intelligence that accentuates the complexities of conventional notion of criminal liability. This study acknowledges the fact that despite of enormous stride of cyber regulatory ecosystem in India, still the changing dynamics of cyberspace calls for erecting a robust institutional infrastructure and legal acclimatization. In the matter of policy perspective, this study recognizes large discrepancy in regulatory enforcement, technological prowess, and transnational partnership. The paper cast a concluding observation in fostering a techno-legal mix of perceptions which ought to imbibe international efforts and capacity building initiatives into legislative

[1] Assistant Professor at ICSS Law College, Bhadrak, Odisha (India). Email: manasmishra0579@gmail.com

 (ISSN: 2583-7753)

reforms. The study put emphasis on arriving at a balanced approach to strengthening cyber security, while upholding fundamental rights of privacy and freedom of expression. Eventually, the paper underlines that to have a meaningful and responsive legal system to cyber-crime; it is highly imperative to revisit the contours of criminal liability in cyberspace.

II. KEYWORDS

Cybercrime, Criminal Liability in Cyberspace, IT Act-2000, Intermediary Liability, Digital Evidence.

III. INTRODUCTION

The invention of the internet and subsequent development of digital technologies have entirely re-organized the socio-economic and legal environment of the world of the present day. This digital era has not only transformed cyberspace into a parallel universe, a borderless, omnipresent new space that is constantly evolving but also offered immense social-economic possibilities and led to the emergence of new more advanced types of criminal activities. Cybercrime in all its many aspects is a threat to the very notions of classic criminal law, specifically, the notions of geographical jurisdiction, physical presence and identifiable offenders.[2]

Historical structuring of criminal law has been mostly developed to suit a world where physical geography prevailed. The appearance of the new sphere of human interaction cyberspace preconditioned the need to re-evaluate the legal concepts, which used to be developed. The traditional concept of the criminal responsibility which is developed based on the provisions of actus reus and mens rea and is implemented in various jurisdictions is ill-fitted to address the issues of cybercrime. Cyberspace crimes do not respect national borders; the representatives of the criminal group work anonymously

[2] Nandan Kamath, *Law Relating to Computers, Internet and E-Commerce* (4th edn, Universal Law Publishing 2014).

and exploit the weaknesses of jurisdiction in ways that are essentially unacceptable by the traditional paradigm of criminal law.[3]

Indian legal reaction to the issue of cybercrime has been a slow but difficult one. The Information Technology Act of 2000 (hereinafter 'IT Act')[4] was an innovative law that dealt with cyber-crimes. Later amendments (especially the one presented by the IT (Amendment) Act, 2008[5] and most recently the introduction of the Bharatiya Nyaya Sanhita, 2023 (hereinafter 'BNS'))[6] have attempted to bring the legal framework in which cybercrime should be regulated into the contemporary arena. Nevertheless, the ever-increasing rate of technological advancements keeps beating the legislation and creates gaps in the law.

The current paper is an expansion of the changing boundaries of criminal responsibility in the cyber space with special regard to the Indian legal system. It discusses the definitional and typological aspect of cybercrime, critically evaluates the current legislative and judicial reaction and outlines the structural and systemic dilemmas, which complicate the successful regulation of cybercrime. In addition, it deals with the transformative implications of new technologies- especially artificial intelligence (AI) - upon criminal responsibility, and suggests a holistic, techno-legal regime of responsible and responsive regulation of cybercrime.

A. Research Objectives

The present study seeks to critically examine the evolving contours of criminal liability in cyberspace within the Indian legal and policy framework. The paper aims to analyse the adequacy of the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 in addressing emerging cyber threats and digital offences. It further intends to evaluate the structural challenges relating to attribution, jurisdiction, intermediary

[3] Vakul Sharma, *Information Technology Law and Practice* (5th edn, Universal Law Publishing 2020).
[4] *Information Technology Act 2000* (No 21 of 2000).
[5] *Information Technology (Amendment) Act 2008* (No 10 of 2009).
[6] *Bharatiya Nyaya Sanhita 2023* (No 45 of 2023).

liability, and admissibility of digital evidence in cybercrime investigations. The study also seeks to examine the impact of artificial intelligence and emerging technologies on conventional doctrines of criminal liability and to propose a balanced techno-legal framework capable of strengthening cybersecurity while preserving constitutional rights and civil liberties.

B. Research Questions

The present study is guided by the following research questions:

1. Whether the existing Indian legal framework adequately addresses the evolving nature of cybercrime and criminal liability in cyberspace?
2. What are the principal legal and jurisdictional challenges involved in attributing criminal liability for cyber offences?
3. How do intermediary liability regimes and digital evidentiary requirements affect cybercrime regulation and enforcement in India?
4. To what extent do emerging technologies such as artificial intelligence and blockchain challenge traditional principles of criminal law?
5. What techno-legal and institutional reforms are necessary for developing an effective and constitutionally balanced cybercrime governance framework in India?

C. Research Methodology

The present study adopts a doctrinal and analytical method of legal research. The research is primarily based on the examination of statutory provisions including the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Bharatiya Sakshya Adhiniyam, 2023, and other relevant regulatory frameworks governing cyberspace and cybercrime in India. The study further relies upon judicial decisions rendered by the Supreme Court of India and various High Courts concerning cybercrime, intermediary liability, digital privacy, and electronic evidence. Secondary sources

including books, journal articles, policy reports, governmental publications, and international instruments such as the Budapest Convention on Cybercrime have also been consulted. Wherever necessary, a comparative perspective has been adopted to analyse international approaches towards cybercrime regulation and emerging technological challenges. The scope of the study is confined to legal and policy dimensions of criminal liability in cyberspace with particular reference to the Indian context.

IV. CONCEPTUALIZING CYBERCRIME: DEFINITION, TYPOLOGY AND CHARACTERISTICS

Conceptual definition of cybercrime is a developing and disputable field of law. The broadest meaning of the term is that cybercrime is any crime where a computer or a network is the means of the crime, the object of the crime, or the locality of the crime. The United Nations office on drugs and crime (UNODC) has stipulated cybercrime to be a crime against or involving the use of a computer, computer system or computer network, crime against the confidentiality, integrity and availability of computer data and computer systems, computer related crime and content related crime.[7]

There are several axes in which cybercrime can be categorized taxonomically. The best international instrument on cybercrime is the council of Europe convention on cybercrime (2001) that categorizes crimes into four: offences against confidentiality, integrity and availability of computer data and systems; computer related offenses; content related offenses and offences against violations of copyright and related rights. The Indian jurisprudence, the IT Act, 2000, refers to a functional taxonomy of hacking, identity theft, cyber fraud, cyberstalking, child pornography and cyber terrorism, among others.[8]

[7] Susan Brenner, *Cybercrime and the Law: Challenges, Issues, and Outcomes* (Northeastern University Press 2012).
[8] David S Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity Press 2007).

The main distinction between cybercrime and traditional crime is the unique phenomenological character of the former. Cybercrime is transnational, i.e. it can be committed in any location around the world and victims anywhere around the world. Anonymity is also a feature as digital technologies enable criminals to conceal their identities using proxy servers, the dark web, and encrypted transactions with currency. The technical nature of cybercrime whereby a single criminal may victimize millions of individuals simultaneously and the fact that it can be scaled only contributes to the challenge of having a response to the crime effectively. All these peculiarities precondition the essential nature of the issue of applying the traditional criminal law doctrines.

V. THE LEGAL FRAMEWORK GOVERNING CYBERCRIME IN INDIA

A. The Information Technology Act, 2000 and Its Amendments

The primary legal instrument governing the actions of the cyberspace in India is the Information Technology Act, 2000, that came into force as a response to the United Nations Model Law on Electronic Commerce (1996). The primary purpose of the conceptualization of the Act was to allow electronic commerce and provide legal acknowledgement to the electronic transactions. Its criminal law, contained in Chapter XI, was largely an afterthought and not a well-considered penal system. Under the first variant of the Act, the crimes that were characterized and penalized were tampered with computer source documents (Section 65), computer systems hacking (Section 66), and the electronic form of obscenity (Section 67).

With the Information Technology (Amendment) Act, 2008 criminal provisions have expanded tremendously to the parent Act. New crimes were introduced by the Amendment, including sending offensive messages through communication service (Section 66A, subsequently declared invalid in Shreya Singhal v. Union of India, (2015) 5 SCC 1), identity theft (Section 66C), cheating by impersonation using computer resources (Section 66D), violation of privacy (Section 66E), cyber terrorism (Section 66F).

The IT Act, though progressive, has been met with a lot of criticism because of the lack of specificity in definition, inadequate sentencing regime, and failure to keep pace with new cyber threats. The definition of the term computer under the Act has been said to be too broad, and may in fact cover digital watches and smart appliances, and its definition of the term hacking as the intent to obtain the wrongful gain or loss has been said to be too broad to cover the variety of cases of unauthorized access. Growing concerns have also been raised over the procedural guidelines of the Act, particularly in searches and seizure of electronic evidence which is thought to be inadequate in terms of cloud computing and distributed storage architecture.[9]

B. The Bharatiya Nyaya Sanhita, 2023: A Critical Appraisal

One significant change in the criminal law in India has been the replacement of the Indian Penal Code, 1860[10], with the Bharatiya Nyaya Sanhita, 2023. The BNS has attempted to incorporate cyber-related dimensions within the broader framework of criminal law, thereby recognising that cybercrime is no longer a specialised regulatory concern but an integral component of the contemporary criminal justice system. The legislation introduces provisions concerning organised crime (Section 111), terrorist acts (Section 113), and offences under Section 152 relating to acts endangering the sovereignty, unity and integrity of India, including activities facilitated through digital platforms and online communication networks. Unlike the erstwhile Section 124A of the Indian Penal Code relating to sedition, Section 152 of the BNS adopts comparatively narrower terminology and does not expressly criminalise mere criticism of the Government, though concerns regarding its potential application in digital contexts continue to invite legal and constitutional scrutiny.

The BNS has, however, been faulted with its failure to comprehensively address the special problems of cybercrime. Skeptics have asserted that the legislative drafters have not properly consulted with the technical specificity required to have effective cybercrime

[9] David S Wall, *Cybercrime: The Transformation of Crime in the Information Age* (Polity Press 2007).
[10] *Indian Penal Code 1860* (No 45 of 1860) (repealed).

laws, and that the incorporation of cyber dimensions to the general criminal law provisions, rather than establishment of specialized cyber penal code, could present interpretive challenges. The fact that the BNS provisions overlap with the IT Act, raises the question of legislation overlapping and the chances of an intersection in the application of the two.

C. Judicial Development of Cybercrime Jurisprudence

The jurisprudence of cybercrime in India has gradually evolved through a series of significant judicial pronouncements addressing digital evidence, intermediary liability, online speech, and privacy concerns. One of the earliest and most important decisions was State of Tamil Nadu v. Suhas Katti (2004), which is widely recognised as India's first conviction under the Information Technology Act, 2000. The case involved the circulation of obscene and defamatory content through an online discussion forum and demonstrated the practical challenges associated with collection, authentication, and admissibility of electronic evidence in cybercrime prosecution. The decision marked an important stage in the judicial recognition of electronic records and digital investigative techniques within the Indian criminal justice system.

A landmark case in the history of Indian cyber law jurisprudence, the case of Shreya Singhal v. Union of India (2015) when the Supreme Court struck down as unconstitutional under the grounds of vagueness and overbreadth such regulation as Section 66A of the IT Act was a landmark case in judicial interpretation of the importance of the freedom of expression in the digital age. The case established some useful precedents regarding the need to be specific with cyber-criminal laws and the need to weigh the concerns of safety against the rights of the civil.[11]

The historic ruling in the case of K.S. Puttaswamy v. Union of India (2017)[12] by the Supreme Court that informational privacy is a constitutional right under the Article 21 of

[11] Jonathan Clough, *Principles of Cybercrime* (2nd edn, Cambridge University Press 2015).
[12] *K S Puttaswamy v Union of India* (2017) 10 SCC 1.

the Constitution has far-reaching implications on cybercrime law. The decision provides that legislative and executive measures around cybercrime must meet the tripartite test of legality, necessity, and proportionality. This constitution does a lot to limit the legislative space within which cybercrime can be codified and puts the State in a positive obligation so that citizens are not exposed to cyber privacy invasion.

VI. STRUCTURAL CHALLENGES IN ESTABLISHING CRIMINAL LIABILITY IN CYBERSPACE

A. Attribution and Identity in Cyberspace

The fundamental problem of establishing criminal liability in cyberspace begins with the problem of attribution that is the technical and legal process of establishing the human actor of a cyber offence. The process of attribution of cybercrime is highly technical and in contrast to traditional crimes where the perpetrator is physically present during the crime, the physical presence of the perpetrator at the scene of the crime provides a prima facie case of identity. Through virtual private networks (VPNs), proxy servers, onion routing (Tor), and cryptocurrency transaction obfuscation, among others, anonymization technologies are frequently deployed by offenders to conceal their identities on the Internet and their locations.

The law of actus reus that requires a recognizable agent to have committed a physical act is seriously contested in the cyber space where acts can be executed through automated scripts, botnets or a third-party computer or device that has been compromised. Attribution has also become more difficult due to the creation of malware-as-a-service and ransomware-as-a-service on dark web markets that create greater separation among malicious software developers, distributors and deployers. Identity in cases of cybercrime has become an issue of concern among the courts in India, and circumstantial digital evidence such as IP addresses, device prints, and records of digital transactions has often been relied upon, whose validity and definitive character is controversial.

B. Jurisdictional Complexity in Transnational Cyber Offences

Perhaps the most intractable issue in regulating cybercrime is jurisdictional complexity. The inherent character of cyberspace as having no borders essentially compromises the principle of territory, on which the traditional jurisdiction of a crime is based. The most common transnational cybercrime situation is where the offender might be based in Country A, using servers in Countries B and C, against victims in Country D, and laundering money through financial systems in Countries E and F. The definition and the evidentiary level, the investigative authority, and the extradition provisions may be different in each jurisdiction, forming an almost impossible maze of jurisdictional complexity.

Section 75 of the IT Act applies Indian jurisdiction to any offence committed by any individual anywhere in the globe provided the offence is a computer offence, computer system or computer network in India. Although this extraterritorial provision represents a progressive legislative interest, in practice this provision is severely limited by the lack of bilateral and multilateral mutual legal assistance treaties (MLATs), aversion of foreign states to cooperate in cybercrime investigations and technical challenges of gathering evidence across the border. India is not a signatory to the Budapest Convention on Cybercrime, the main multilateral tool in international cooperation on cybercrime, and this absence is a big impediment to India being able to effectively engage in transnational cybercrime prosecution.[13]

C. Intermediary Liability and the Safe Harbour Conundrum

One of the most contentious questions in the law of cybercrime with the most far-reaching implications is the question of intermediate liability. Internet service providers (ISPs), social media, search engines, and cloud service providers are key actors in the cyberspace ecosystem as regulators of digital communication and commerce. The extent to which

[13] Markus Rauschecker, *Cybercrime and Jurisdiction: A Global Survey* (TMC Asser Press 2006).

these entities can be criminally or civilly liable to illegally enabled content that has been facilitated by their platforms raises deep legal, economic, and policy questions[14].

Section 79 of the IT Act, as amended in 2008, provides conditional immunity or "safe harbour" protection to intermediaries against liability arising from third-party content hosted on their platforms, subject to compliance with prescribed due diligence obligations and lawful takedown requirements. The development of this safe harbour framework was significantly influenced by the decision in Avnish Bajaj v. State (2005), popularly known as the Bazee.com case.

The case arose from the listing of obscene material for sale on an online marketplace platform, resulting in criminal proceedings against the platform's Managing Director. The Delhi High Court's observations in the case highlighted the legal uncertainty surrounding intermediary liability under the pre-amendment framework and substantially contributed to the later introduction of Section 79 safe harbour protections through the Information Technology (Amendment) Act, 2008. Such responsibilities were further elaborated in the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which included traceability of originator of messages, periodic reporting of compliance and appointment of grievance officers.[15]

The traceability requirement under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 has generated significant constitutional debate, particularly on the ground that mandatory traceability may undermine end-to-end encryption used to secure digital communications of journalists, activists, and ordinary users. The issue reflects the continuing tension between the State's interest in investigating cyber offences and the constitutional right to privacy recognised in K.S. Puttaswamy v. Union of India. The constitutional validity and scope of traceability requirements presently remain subject to adjudication before the Supreme Court in

[14] Pavan Duggal, *Cybercrime Investigations in India* (Saakshar Law Publications 2018).
[15] Debarati Halder and K Jaishankar, 'Cyber Crimes against Women in India: Issues, Policy and Prevention' (2011) 6(1) *Sri Lanka Journal of International Law* 141.

Antony Clement Rubin v. Union of India[16], which originated before the Madras High Court and was subsequently transferred to the Supreme Court. Consequently, observations made during the Madras High Court proceedings may only be treated as preliminary in nature and not as a final judicial determination on the legality of traceability obligations.

D. Evidentiary Challenges in Digital Forensics

The admissibility and credibility of digital evidence constitute a significant challenge in the prosecution of cybercrime. The Indian Evidence Act, 1872 was originally ill-equipped to address electronic evidence and was subsequently amended by the Information Technology Act, 2000, which through its Second Schedule inserted Section 65B relating to the admissibility of electronic records. An authoritative interpretation of the requirements governing electronic evidence was subsequently provided by the Supreme Court in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020), wherein the Court clarified that the certificate requirement under Section 65B (4) is mandatory and not merely procedural in nature.

However, the existing evidentiary framework is severely questioned in the framework of modern cybercrime investigations. The volatility of digital evidence, which can be easily altered, deleted or faked, demands a robust chain-of-custody documentation and evidence collection methods that are not only forensically valid but also comprehensive. The proliferation of cloud computing whereby information can be shared among multiple servers across multiple jurisdictions brings forth unprecedented evidence of preservation and retrieval challenges. In addition, the recent framework is ineffective at dealing with new forms of evidentiary puzzles presented by the new use of blockchain-based systems, encrypted communications, and decentralized applications. The Indian Evidence Act has since been replaced by the new Bharatiya Sakshya Adhiniyam, 2023, which has introduced new requirements on electronic evidence, although it is yet to be

[16] *Antony Clement Rubin v. Union of India, Transfer Case* (Civil) No. 189 of 2020 (Supreme Court of India, pending).

determined whether the requirements are sufficient to address the difficulties of determining the issue of modern cybercrime.[17]

VII. ARTIFICIAL INTELLIGENCE AND THE TRANSFORMATION OF CRIMINAL LIABILITY

One of the most significant changes in the contemporary cybercrime landscape is the emergence of artificial intelligence as an instrument of committing cybercrimes, along with becoming a victim of cyberattacks. The qualitatively new layers of the issue of criminal liability introduced by the AI-based cybercrime are clearly something that the existing criminal justice system is clearly unprepared to address. The use of AI in cybercrime may be perceived in different ways: deepfakes generated by AI may be used to commit financial fraud and identity theft; phishing campaigns that are enhanced by AI can be used to create highly personalized and linguistically advanced frauds; autonomous malware can also be used, and machine learning is implemented to avoid security measures; social engineering attacks powered by AI can be used to exploit the psychological vulnerabilities on a scale never seen before

There are fundamental conceptual issues with the application of traditional criminal law principles to AI-enhanced cybercrime. One of the fundamental premises of the doctrine of mens rea which requires the evidence of an actor who is in a guilty mental state or criminal intent is the assumption of a human actor being able to engage in subjective states of mind. Whether the mental state of the person who has realized the requirement of the mens rea is duly met or not becomes a reality question in case the criminal act is carried out by an independent AI system, which has no direct human instruction, i.e., autonomous trading algorithms that have unintentionally committed a market manipulation or self-educated malware that has autonomously identified a vulnerability and used it. None of the candidates mentioned above can be interpreted in the paradigm

[17] Gurshabad Grover, 'Regulating Social Media Intermediaries: A Study of the IT Rules, 2021' (2021) 13(2) *NUJS Law Review* 1.

of a classic mens rea: the creator of the AI-system, the deployer, the operator, or the system.[18]

The issue of deep-fake technology is particularly serious to existing legislation. The IT Act does not specifically address crimes related to deepfakes but the provisions on identity theft (Section 66C), cheating by personation (Section 66D) and obscenity (Sections 67, 67A, 67B) can be interpreted to address certain forms of deepfake abuse. The BNS, 2023, has no specific provisions regarding AI-generated synthetic media, but the offences that are facilitated by deepfakes, like non-consent intimate image abuse, political misinformation, and financial fraud, are a rapidly expanding form of cyber-crime. The legislation gap in the field is a matter to be considered.

The issue of negligence, strict liability, and vicarious liability is relevant in regard to the AI developer and deployer liability towards the crimes committed with the assistance of their systems. The application of a product liability model of AI systems which makes it possible to commit crimes has also been suggested by other researchers, as is the case with the liability of the manufacturers of arms that make it possible to commit violence. Other proposals have been put forward that a concept of such organizational criminal liability does exist, and corporations that develop or utilize AI systems must be criminally liable when they have failed to institute reasonable preventive steps that can be anticipated against criminal misuse. These theoretical models are however not highly embraced in the Indian positive law and their development through judicial interpretation or legislation is still crucial.

VIII. EMERGING CYBER THREATS AND THE INADEQUACY OF THE EXISTING FRAMEWORK

The cyber threat environment is dynamic, and change has continued to be high and has far outpaced the efforts of legislatures and regulation. Ransomware has been one of the

[18] NS Nappinai, 'Cyber Crime Law in India: Has Law Kept Pace with Emerging Trends? An Empirical Study' (2010) 8 *Journal of International Commercial Law and Technology* 22.

most prevalent and the costliest forms of cybercrime which is malicious software that encrypts data of its victims and demands payment of decryption keys. In India, critical infrastructure, including hospitals, government agencies, and financial institutions, has been targeted with ransomware in India, CERT-In has indicated that ransomware attacks have grown exponentially over the last few years. The existing provisions of the IT Act though technically applicable about ransomware under Sections 43, 66 and 66B provide inadequate deterrence as ransomware crimes are normally transnational, and it is hard to enforce the law in the country.[19]

Cryptocurrency and blockchain technologies have introduced new dimensions to cybercrime both as instruments facilitating unlawful activities and as targets of cyberattacks. Cryptocurrency transactions are largely pseudonymous in nature, thereby contributing to the growth of darknet markets, ransomware payment systems, and digital money laundering operations. Further, the decentralised architecture of blockchain networks limits conventional law enforcement intervention because of the absence of a central regulatory authority capable of freezing or reversing transactions. Although the Cryptocurrency and Regulation of Official Digital Currency Bill, 2021 was proposed as a legislative initiative, the Bill was never enacted and is no longer pending consideration. In the absence of a dedicated statutory framework, India has instead adopted a limited taxation-based approach through the Finance Act, 2022, including taxation on gains arising from virtual digital assets. Nevertheless, the continued absence of a comprehensive regulatory framework governing cryptocurrencies and blockchain transactions creates significant legal and enforcement gaps that may be exploited for cybercrime, financial fraud, and illicit digital transactions.

The advent of the Internet of Things (IoT) is a novel form of cyber vulnerability to which the existing legal framework is ill-equipped to address. The internet-related explosion of devices, both in smart homes (appliances), and in industrial control systems and critical

[19] Ryan Calo, 'Robotics and the Lessons of Cyberlaw' (2015) 103(3) *California Law Review* 513.

infrastructure, has significantly expanded the attack surface presented to cybercriminals. Security vulnerabilities associated with IoT, including default credentials, weak and out-of-date firmware and poor communication protocols, have been frequently exploited to execute distributed denial-of-service attacks, surveillance, and sabotage of industrial systems. The Indian legal provisions on the security of the IoT are still in its infancy and there is no specific law that is proceeding in connection with the security of the IoT devices and liability of manufacturers of the IoT devices in case of any security breach.[20]

IX. INTERNATIONAL FRAMEWORKS AND COMPARATIVE PERSPECTIVES

The multilateral tools, regional initiatives, and bilateral treaties have served as a variety of global tools that have helped the global community deal with the issue of cybercrime. The broadest multilateral cybercrime treaty is the Budapest Convention on Cybercrime (2001) that was adopted by the Council of Europe and open to non-member states. The Convention provides substantive and procedural guiding principles to cybercrime laws which include substantive criminal offences, procedural powers of investigation and prosecution and systems of international cooperation. As of January 2024, the Budapest Convention on Cybercrime had 69 State Parties, while several additional jurisdictions have relied upon its principles as persuasive guidance for developing domestic cybercrime legislation and international cooperation mechanisms.

The fact that India has not ratified the Budapest Convention is a significant aberration in Indian international cooperation in fighting cybercrime. Though, India has signed bilateral cybersecurity cooperation agreements with certain states, including the United States, the United Kingdom, and members of the QUAD grouping, none of the agreements have the multilateral framework to convict transnational cybercrime. The international legal framework governing cybercrime has undergone a significant development with the adoption of the United Nations Convention against Cybercrime

[20] Jack Goldsmith and Tim Wu, 'Digital Borders' (2006) *Legal Affairs* 40.

by the United Nations General Assembly through Resolution 79/243 on 24 December 2024. The Convention constitutes the first comprehensive and legally binding global treaty specifically addressing cybercrime and the criminal misuse of information and communication technologies.

Unlike the Budapest Convention on Cybercrime, which originated as a regional Council of Europe instrument and was subsequently opened to non-member states, the UN Convention seeks to establish a broader multilateral framework with wider participation from developing and Global South countries, including greater emphasis on sovereignty, international cooperation, digital evidence sharing, and capacity building. The Convention also attempts to harmonise substantive cybercrime offences, procedural mechanisms for investigation, and mutual legal assistance obligations among State parties. India's position regarding accession or ratification of the Convention assumes considerable significance in the context of transnational cybercrime governance. Although India has historically refrained from acceding to the Budapest Convention on grounds relating to sovereignty and limited participation in its drafting process, the adoption of the UN Convention presents a new opportunity for India to engage within a globally negotiated multilateral cybercrime framework. The extent to which India aligns its domestic cybercrime laws and institutional mechanisms with the obligations contemplated under the Convention will substantially influence the effectiveness of future international cooperation in cybercrime investigation, extradition, and digital evidence enforcement.[21]

Indian regulatory reform in comparison is learning some lessons regarding cybercrime that are being offered by the legislative approach used by the European Union. The EU Network and Information Security (NIS) Directive and its successor directive NIS2 Directive establish extensive security obligations on the operators of essential services and digital service providers that are reinforced by the threat of substantial

[21] Bert-Jaap Koops and Miriam Cushman, 'Criminal Law, Technology and the Interface Between the Physical and the Virtual' (2013) 26(3) *International Journal of Law and Information Technology* 191.

administrative penalties in case of breach. Another new system of data protection with colossal cybercrime consequences is the EU General Data Protection Regulation (GDPR). The experience of the EU in regulating AI, including the AI Act, in which the AI application is classified according to its risk assessment and exerted more or less pressure on the regulation system, may serve as a possible source of information on how AI regulation in India can be conducted since the AI regulation system is rather young there.

X. POLICY DIMENSIONS AND INSTITUTIONAL FRAMEWORK

Indian system of governance of cybercrime is typified by a complex institutional structure comprising of several regulatory agencies, law enforcement agencies and quasi-judicial institutions. The primary institutional stakeholders include the Ministry of Electronics and Information Technology (MeitY), CERT-In, National Cyber Security Coordinator, the Cyber Crime Coordination Centre (I4C) of the Ministry of Home Affairs and special cyber-crime investigation units established by state police forces. The reason is that it is the multi-faceted nature of cybercrime that gives rise to this multiplicity of institutional actors that has resulted in a challenge of coordination, which impedes the successful enforcement of regulations.

The National Cyber Security Policy, 2013 constituted India's first comprehensive policy framework on cybersecurity and sought to promote the protection of critical information infrastructure, development of cybersecurity capabilities, and enhancement of cyber awareness. However, the Policy was frequently criticised for the absence of concrete implementation mechanisms, measurable institutional accountability, and coordinated enforcement structures. In response to evolving cyber threats and rapid technological transformation, India formally launched the National Cybersecurity Strategy 2026 in February 2026 to establish a more comprehensive and operational cybersecurity governance framework.

The Strategy emphasises the protection of critical digital infrastructure, strengthening cyber incident response systems, enhancement of digital forensics capabilities, development of specialised cybercrime investigation mechanisms, public-private

cooperation, and capacity building in cybersecurity education and research. The Strategy also recognises emerging threats arising from artificial intelligence, ransomware, cloud computing, and Internet of Things (IoT) ecosystems. Nevertheless, despite its broader institutional vision, concerns remain regarding the practical implementation of the Strategy, particularly in relation to regulatory oversight of AI-enabled cybercrime, standardisation of IoT security obligations, cross-border digital evidence collection, and coordination among multiple cybersecurity agencies.

Consequently, while the National Cybersecurity Strategy 2026 marks an important advancement in India's cyber governance framework, its long-term effectiveness will depend upon legislative harmonisation, institutional capacity building, and sustained technological adaptation.[22]

Institutional capacities to investigate and prosecute cybercrime is one of the biggest gaps in the Indian system of governance of cybercrime. Most of the state police lack trained and equipped cybercrime investigation units. Poor laboratory facilities, untrained digital forensic examiners, and standard forensic processes are some of the shortcomings that hinder the forensic analysis of digital evidence. The fact that the judicial officers are not conversant with the technicalities of digital evidence has also been a hindrance to cybercrime, and thus much must be done to invest in judicial capacity building and training.

One of the key changes in the legal sphere that has vital implications on the cybercrime system is the Digital Personal Data Protection Act, 2023 (DPDPA) that took effect in August 2023. The Act contains a comprehensive framework of personal data protection and the responsibilities of data fiduciaries and data processors, rights of data principals and the Data Protection Board of India enforcement. The data breach provisions of the Act (the notification to the Board and the affected individuals in case of unauthorized

[22] Pavan Duggal, 'Legal Issues in AI and Blockchain' (2019) *International Journal of Law and Technology* 45.

access to personal data) can be directly used in cybercrime and is complementary to the existing framework of the IT Act.

XI. SUGGESTIONS AND RECOMMENDATIONS

The foregoing analysis demonstrates that the existing cybercrime framework in India requires comprehensive legislative, institutional, and technological reforms to effectively address the rapidly evolving nature of cyber threats. In this context, the following suggestions and recommendations are proposed to strengthen cybercrime governance while ensuring constitutional safeguards relating to privacy, freedom of expression, and due process.[23]

1. India should enact a comprehensive and technology-neutral Cybersecurity and Cybercrime Code consolidating scattered provisions presently contained under the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and allied regulatory frameworks. Such legislation should specifically address emerging offences involving artificial intelligence, deepfakes, ransomware, cryptocurrency-based crimes, and Internet of Things (IoT) vulnerabilities while prescribing clearer standards for attribution of liability, intermediary accountability, and digital evidence collection.[24]
2. institutional reforms must be undertaken through the establishment of specialised National Cybercrime Investigation Units, dedicated Cyber Forensics Laboratories, and technologically trained judicial benches for cyber-related offences. Regular technical training programmes should also be introduced for police authorities, prosecutors, and judicial officers to improve the handling of digital evidence and cybercrime prosecution.

[23] Tanvir Ahmad Khan, 'Cybercrime and Criminal Liability in India: Critical Appraisal of IT Act, 2000' (2017) 3(2) *International Journal of Law and Legal Jurisprudence Studies* 156.
[24] Aparna Viswanathan, 'Intermediary Liability in India: The IT (Amendment) Act, 2008 and the Intermediary Guidelines Rules, 2011' (2011) 7 *International Journal of Law and Technology* 97.

3. India should strengthen international cooperation mechanisms by actively participating in multilateral cybercrime frameworks and expanding bilateral mutual legal assistance arrangements for cross-border cyber investigations and evidence sharing. In this regard, India may reconsider its position regarding broader participation in international cybercrime treaty frameworks to improve transnational enforcement capabilities.[25]

4. cybercrime governance must maintain an appropriate balance between national security and civil liberties. Any surveillance, traceability, or intermediary compliance mechanism should conform to the constitutional principles of legality, necessity, and proportionality recognised in K.S. Puttaswamy v. Union of India. Simultaneously, long-term investment in cybersecurity education, public digital literacy programmes, and public-private partnerships is necessary for strengthening India's institutional resilience against cyber threats and ensuring sustainable cyber governance in the digital era.

XII. CONCLUSION

The present paper has traced the shifting frontiers of criminal responsibility in cyberspace by demonstrating that the revolution created by digital technologies has fundamentally doubted the dogmatic assumptions of conventional criminal law. The analysis has shown that the existing legal framework of cybercrime in India, the majority of which consists of the IT Act, 2000, and the BNS, 2023, despite being indicative of progressive law-making practices, has multiple gaps and organizational deficiencies that prevent the effective enforcement of cybercrime laws in the contemporary digital environment.

Structural issues that cannot be tackled with either separate legislative change or case-by-case judicial interpretation include the attribution of issues, the complexity of jurisdiction, intermediary liability, and the digital evidentiary standards. They need

[25] Yoti Rattan, 'Cyber Crimes and Its Classification' (2015) 14(2) *Journal of Computer Science and Technology* 56.

rather radical re-conceptualization of the fundamental concepts of criminal liability reus, mens rea, causation and complicity in cyberspace because of the ontological and phenomenological peculiarities of cyberspace. This reevaluation must be grounded in an ideological engagement with constitutional values, in particular, the right to privacy and freedom of expression and be mindful of the risk of the State going too far in the cause of cybersecurity.

The introduction of artificial intelligence as the method and instrument of cybercrime introduces qualitatively new problems, which the existing order is obviously unprepared to oppose. The next urgent topic of legislative intervention is the establishment of a uniform legal framework to address the problem of AI-assisted cybercrime liability, which provides the answer to the question of developer, deployer, and operator liability by combining both the fault-based and strict liability liabilities.

Lastly, cybercrime governance in India needs to be comprehensive in nature and should undergo techno-legal response which involves legislative reform, capacity building in institutions, international cooperation and constitutional faithfulness. It should be admitted that the rule of law in the era of the digital world must be technologically informed and must not be technologically seized and that the necessity of the State to protect citizens against cybercrime must also be supported with the corresponding necessity to protect citizens against the possibility of the State itself to use digital surveillance and enforcement powers abusively. Not only is this balance a matter of regulation but a matter in itself is the problem of the quality and viability of the Indian constitutional order of democracy in the digital age.

XIII. REFERENCES

A. Statutes and Legislation

1. The Information Technology Act, 2000 (No. 21 of 2000).
2. The Information Technology (Amendment) Act, 2008 (No. 10 of 2009).

3. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
4. The Bharatiya Nyaya Sanhita, 2023 (No. 45 of 2023).
5. The Bharatiya Sakshya Adhiniyam, 2023 (No. 47 of 2023).
6. The Digital Personal Data Protection Act, 2023 (No. 22 of 2023).
7. The Indian Penal Code, 1860 (No. 45 of 1860) [now repealed].
8. The Indian Evidence Act, 1872 (No. 1 of 1872) [now repealed].
9. Council of Europe, Convention on Cybercrime (Budapest Convention), CETS No. 185 (2001).
10. European Union, General Data Protection Regulation (EU) 2016/679.

B. Cases

1. Shreya Singhal v. Union of India, (2015) 5 SCC 1.
2. K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
3. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
4. Antony Clement Rubin v. Union of India, W.P. (MD) No. 8358 of 2020 (Madras HC, 2021).
5. State of Tamil Nadu v. Suhas Katti, (2004) Cri LJ 4541.
6. Avnish Bajaj v. State, (2005) 116 DLT 427.

C. Books and Monographs

1. Nandan Kamath, Law Relating to Computers Internet & E-Commerce (4th edn., Universal Law Publishing, 2014).
2. Vakul Sharma, Information Technology Law and Practice (5th edn., Universal Law Publishing, 2020).
3. Rodney D. Ryder, Guide to Cyber Laws (Wadhwa & Co., 2012).

 (ISSN: 2583-7753)

4. Susan Brenner, Cybercrime and the Law: Challenges, Issues, and Outcomes (Northeastern University Press, 2012).
5. David S. Wall, Cybercrime: The Transformation of Crime in the Information Age (Polity Press, 2007).
6. Jonathan Clough, Principles of Cybercrime (2nd edn., Cambridge University Press, 2015).
7. Thomas J. Holt, Adam M. Bossler & Kathryn C. Seigfried-Spellar, Cybercrime and Digital Forensics: An Introduction (2nd edn., Routledge, 2018).
8. Markus Rauschecker, Cybercrime and Jurisdiction: A Global Survey (T.M.C. Asser Press, 2006).
9. Pavan Duggal, Cybercrime Investigations in India (Saakshar Law Publications, 2018).

D. Journal Articles

1. Debarati Halder & K. Jaishankar, 'Cyber Crimes against Women in India: Issues, Policy and Prevention' (2011) 6(1) Sri Lanka Journal of International Law 141.
2. Gurshabad Grover, 'Regulating Social Media Intermediaries: A Study of the IT Rules, 2021' (2021) 13(2) NUJS Law Review 1.
3. N.S. Nappinai, 'Cyber Crime Law in India: Has Law Kept Pace with Emerging Trends? An Empirical Study' (2010) 8 Journal of International Commercial Law and Technology 22.
4. Ryan Calo, 'Robotics and the Lessons of Cyberlaw' (2015) 103(3) California Law Review 513.
5. Jack Goldsmith & Tim Wu, 'Digital Borders' (2006) Legal Affairs 40.

6. Bert-Jaap Koops & Miriam Cushman, 'Criminal Law, Technology and the Interface Between the Physical and the Virtual' (2013) 26(3) International Journal of Law and Information Technology 191.
7. Pavan Duggal, 'Legal Issues in AI and Blockchain' (2019) IJLT 45.
8. Tanvir Ahmad Khan, 'Cybercrime and Criminal Liability in India: Critical Appraisal of IT Act, 2000' (2017) 3(2) International Journal of Law and Legal Jurisprudence Studies 156.
9. Aparna Viswanathan, 'Intermediary Liability in India: The IT (Amendment) Act, 2008 and the Intermediary Guidelines Rules, 2011' (2011) 7 IJLT 97.
10. Yoti Rattan, 'Cyber Crimes and Its Classification' (2015) 14(2) Journal of Computer Science and Technology 56.

E. Reports and Online Sources

1. CERT-In, 'Annual Report 2022–23' (Indian Computer Emergency Response Team, Ministry of Electronics and Information Technology, 2023).
2. Ministry of Home Affairs, 'Annual Report of National Crime Records Bureau: Cyber Crime Statistics' (2022).
3. Internet and Mobile Association of India (IAMAI), 'Digital India Report' (2023).
4. National Cyber Security Policy, 2013 (Ministry of Communications and Information Technology, Government of India).
5. Law Commission of India, 'Report No. 221 – Need for Legislation for Regulation of Electronic Commerce' (2009).
6. Council of Europe, 'Guidance Note on Intermediary Liability and Freedom of Expression Online' (2020).
7. Europol, 'Internet Organised Crime Threat Assessment (IOCTA) 2023' (European Union Agency for Law Enforcement Cooperation, 2023).

8. ITU, 'Global Cybersecurity Index 2020' (International Telecommunication Union, 2021).
9. Interpol, 'ASEAN Cyberthreat Assessment 2021' (International Criminal Police Organization, 2021).