Page 1616 – 1624 **DOI:** *https://doij.org/10.10000/IJLMH.1111669*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 2

2026

Critical Evaluation of India's Cybercrime Framework

SATVIK SHARMA[1]

ABSTRACT

The swift penetration of digital technologies along with the Internet has metamorphosed India into one of the fastest growing digital economies. Such a transformation has generated an increasing offensive response to the recruiting of various malfeasance, like hacking, identity theft, phishing, cyberstalking and financial fraud and to finding solutions for the protection of privacy and rights online coherent with the state. To address these threats of cybercrime, India has thrown together a legal framework moving from the Information Technology Act, 2000, the Criminal Law Amendment under the Bharatiya Nyaya Sanhita, 2023, the procedural framework under the Bharatiya Nagarik Suraksha Sanhita, 2023, and the data protection regime introduced through the Digital Personal Data Protection Act, 2023. Put together, these laws aim to regulate cyber activities, criminalize digital offences, and uphold the sanctity of an individual digital presence. The present paper with critical attention evaluates the cybercrime framework in light of the Indian legislative perspective, strengths, and weaknesses, and enforcement modalities, transnational crime, which maintain the cybercrime as an offense. It might be generalized that even though it possesses broad-based legal provisions, India requires continuous legal reforms, sustained enough enforcement institutions, more influential global cooperation and more cordially bonded collaboration.

Keywords: *Cybercrime, Cyber Law, Data Protection, Information Technology Act, Bharatiya Nyaya Sanhita, Digital Personal Data Protection Act.*

I. INTRODUCTION

Digital age has entirely transformed communication, trade, governance, and social interaction. India has seen notable engagements with internet, digital payment services, and online services because of the swell in e-governance campaigns and digital infrastructure. They boost efficiency and connectivity but also open the door to cybercrimes. Cybercrime is a legal term used for crimes carried out digitally against individuals, organizations, or governments. Types of cybercrime comprising online information vices are hacking, email phishing attacks, theft of confidentiality or online fraud, cyber harassment or denial of service attacks, or unauthorized

[1] Author is an LL.M. Student at Amity University, Noida, Uttar Pradesh, India.

 [ISSN 2581-5369]

entry of the computer system. The vast dimension of cyberworld restricts the control and suppression of these crimes. India put together a legislative framework regarding cybercrime because of the growing threat. It consists of cyber security laws in the Information Technology Act, 2000, alongside other criminal laws provided by the Bharatiya Nyaya Sanhita, 2023. Procedures under the Bharatiya Nagarik Suraksha Sanhita, 2023, are meant to provide administrative backup. The Digital Personal Data Protection Act, 2023, is a great achievement as it is the first legal measure taken by India to protect personal data on digital transactions and to have some control over personal digital lives.

II. LEGAL FRAMEWORK GOVERNING CYBERCRIME

Organized cybercrime within India falls within its established statutory regime of regulation. The Information Technology Act, 2000 had wide-ranging applicability for Indian cyberspace and had the specific salient features of its legal recognition of electronic records, digital signatures, with punishments attaching to unauthorized revelation of computer secrecy, the implantation program, cyberfraud, and cyberterrorism. Further, the Act places such liability penalties and compensation, mechanisms for damages upon affected people, who may object to cyber offenses. These legislations have fostered electronic communication and digital transactions, providing a conducive environment for safe online activities. The primary law defining cyber-related offenses is further augmented by the Bharatiya Nyaya Sanhita 2023, which forms other, allied offenses. The BNS addresses crimes such as cheating, fraud, impersonation, and obscenity when done electronically, thereby filling gaps untouched by I. T. Acts. The B. N. S. integrates cyber offences with the broader legal framework whereby those who prey upon computer platforms can be tried under the general laws instead of project-specific cyber legs. Cybercrime Proceedings, viz., the investigatory perspectives, operate under the domain of the Bharatiya Nagarik Suraksha Sanhita 2023, which renders electronic shreds of evidence, written data, and technology as acceptable norms for the purpose of criminal investigation and prosecution. This will help the magistrate, the prosecution, and the defense to understand electronically-produced evidence in cybercrime cases. Moreover, laws in place that ensure data protection and privacy have only been reinforced by the Digital Personal Data Protection Act, 2023, thereafter achieving a legal framework and for collection, storage, or the transmission of personal data to and by organizations and government entities. [2]

[2] Digital Personal Data Protection Act, 2023.

 [ISSN 2581-5369]

III. STRENGTHS OF INDIA'S CYBERCRIME FRAMEWORK

A major strength in India's cybercrime legislation is the enactment of specific laws for digital offenses. The Information and Technology Act affirms a legal framework regulating cyber acts and criminalizes the various issues like hacking, identity theft, and unauthorized access to computer systems. Most importantly, this act has helped to inculcate a sense of digital accountability. Another strength is the integration of cybercrime laws within the nitty-gritty of Andennso's criminal justice system. By enacting some offenses committed through digital platforms within the territoriality of the general criminal law, the well-known XX sticks to the principle of 'equity' as the bona fide prototype. Under the said provision, cyber offenders could be prosecuted when their acts overlap in traditional crimes of fraud, or recession. Digital Personal Data Security Act, 2023 would make the Indian cyber regime even more robust in its privacy and data protection aspects. The Act would hold organizations more accountable concerning personal data; it would further bring back in line the ones liable to legal wrangles pertaining to data subject to misuse or compromising. Perfectly aligned with global benchmarking on privacy, maintaining an ambitious vision to safeguard the personal data of citizens in the digital era of government policy. The procedural reforms of the Bharatiya Nagarik Suraksha Sanhita allow electronic records and digital evidence to be used for investigations in criminal trials. These features bring the justice system up-to-date and provide law enforcement with tools to deal effectively with cyber-related crime.

Cybersecurity specialists find personal data protection increasingly valuable when digital data files are processed with great volume. The PDPA supports conscientious data management practices regulated by CAO for individuals that also raises awareness of data security and accountability among the organizations that are managing personal information. It is instrumental to discovering the criminal nature of evidence during the proceedings before trial. The concept, as laid down by the Cybercrime Act of India, is now called electronic evidence. It helps in the progression of a procedural reform, assisting the prosecution in their collection, preservation, and presentation of digitally veritable information in the trials. The Accountable mechanisms for digital forensics and efficient tools procedures are vital in cybercrime investigation of offenders.[3]

IV. LIMITATIONS AND CHALLENGES IN THE EXISTING FRAMEWORK

India cyber law remains deficient, despite the totality of the legal structure that is reserved for

[3] Bharatiya Nagarik Suraksha Sanhita, 2023 (electronic evidence provisions).

 [ISSN 2581-5369]

cybercrime. One of the major challenges is the lightning-fast pace of technological innovation. Cybercriminals are invariably and incessantly designing and deploying new forms of cyberattacks such as ransomware, cryptocurrency frauds, and AI-based cyber manipulation. Because the existing laws must cope with new threats, one attendant responding comfort seems to be that these-such things are not moderately or well treated by those established laws. Another limitation arises from the sheer technical complexity of cybercrime investigation. Cybercrimes are replete with incredible complexity and are normally woven around the concept of anonymity, tots defense, and multiple electronic storage media technologies. It, in other words, requires the employment of extremely technologically skilled personnel who are well versed in different forms of highly specialized digital forensics. Unfortunately, a sufficient number of the requisite personnel and infrastructure remains lacking with many law enforcement agencies. There are a number of regulatory issues that have been brought home with this balance between privacy protection, cybersecurity, and law enforcement. The Digital Personal Data Protection Act offers for the protection of personal data, but on the other end, law enforcement may stand in need of access to some kind of digital information during cybercrime investigations. Balancing these purposes with unreserved subject rights to privacy is problematic and legal issue.[4]

Issues related to legal stipulations, which are much needed to overlay a sense of institution over cyberspace, are lamentable. Technology has always been in advance and merely one step or sometimes a mile ahead of contemporary laws. As such, cybercriminals, in pursuit of carrying out wrongful deeds, make use of ultra-modern technologies like AI or machine learning, all of which work against giving valuable insights to the mere hunting and capture of the ghost that initiated the attacks. On the one hand, with 2000's Information Technology Act, there's a decent attempt in the regulation of multiple forms of cyber misconduct. On the other, many digital tools we use now do not even exist at the time of the law's passing. Thus, that leaves a bunch of cyber attacks now-Deepfake manipulations, cryptocurrency laundering, and the vast proliferation of ransomware attacks-not clearly caught in the net of laws and frameworkIn digitally transformed India, globalization of transactions-based electronic crimes poses a severe challenge. This shift dispels many prior notions of standard forensics. A deviation also arises from burdens and difficulties in the collection and preservation of digital evidence. The major problem hinges on the conflicting views among different laws and their provisions about cyber phenomena. At the end of the day, it all leads to the safe preservation, labelling, acquisition, and administration of digital research for prosecution purposes in case of an offence. As a matter

[4] Justice B.N. Srikrishna Committee Report on Data Protection.

 [ISSN 2581-5369]

of reality, some could be so contradictory among all the legislations regarding the collection of digital evidence, on one recent couple of occasions, that tales were woven around them, and on the other occasion, facts were distorted more than just a bit. In other situations, it could be different—that another law could be taken into account solely because it casts more light on things. And in extraordinary circumstances, chances arise that none of these implicitly provide any lightening of the picture since each usually creates further confusion. S. 89(b) of the Bharatiya Nagarik Suraksha Sanhita, 2023 specifically provides for the admissibility of the electronic evidence in court: in doing so, however, the law leaves you to guess the fate of the legal credibility, chain of custody, and authentication amid many security threats associated with this evidence. Even then, another limitation concerns the plain overlapping between a number of these existing laws affecting cyber- court.[5] The matter of privacy rights and personal data protection is something of concern. A Digital Personal Data Protection Act, 2023 serves the purpose of strengthening privacy safeguards within the law of India. The effectiveness of this Act will depend to a large extent on mechanisms to enforce privacy rights—the development of regulatory authorities and the institution of processes to guarantee adherence to and respect of appropriate data protection standards by those organizations are the matters requiring serious attention. One looks for a balance between some measure of data protection for personal data, for example, that such data should not be put to public use without the consent of data subjects on one hand, and the possibility to share information with police and enforcement agencies for cybercrime investigations on the other, amongst other issues in the system.[6]

V. CHALLENGES IN ADDRESSING TRANSNATIONAL CYBERCRIME

One transnational characteristic of cybercrime is that digital networks exist beyond our national borders. Interference can be directed easily between victims; some in imports otherwise area. Laboratories are met by limited practical encounters with repeated difficulties crediting dearth of prosecutive efforts using computer savvy on the part of law enforcement personnel. Law enforcement agencies try to break barriers as in the case of the investigation and the prosecution of cyber criminals. These are some of the obstacles inhibiting progress with mutual legal assistance treaties. Synergism in securing mutual mutual collaboration with other relevant entities to fight cybercrime truly entails joint collective work. Inter-governments, law enforcement agencies, and several international organizations (IOs) need to work together to

[5] Information Technology Act, 2000; Bharatiya Nyaya Sanhita, 2023; Digital Personal Data Protection Act, 2023.
[6] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime* (UNODC).

 [ISSN 2581-5369]

advocate the sharing of resources, conduct joint investigations, and harmonize international cyber crime law. Such collaborative efforts are needed to address cybercrimes occurring in different regions around the world threats.[7]

Further interpretational challenges stem from the wide use of encryption technologies in digital communication. Encryption indeed plays a speechless role in ensuring secrecy and security for online transactions; however, on the flip side, this draws in misbehavior from cybercriminals. The use of encrypted communications apps and secure platforms to communicate often blocks any crucial evidence that would assist law enforcement bodies in battling cybercrimes. Where the legal framework does admit law enforcement agencies access to relevant data, the formidable strength of the established channeled encryption might erode the functioning of such legal provisions. The quest for privacy at the expense of going after cybercrimes, therefore, remains the prime policy dilemma challenge.[8] When investigating cyber crimes, attempts are rated complex due to involvement of numerous technology trends and service providers. Cyber crimes have also crossed borders and involve entities that could include internet service providers, cloud storage companies, social media platforms, and financial institutions based in diverse jurisdictions. The interaction with such entities to secure valid digital evidence can be difficult and time-consuming at times. Procedures were put in place for obtaining formal access to the information, as the need for effective law enforcement must be weighed against privacy rights; this, in turn, can sometimes halt investigations.

It is manifest that this relatively new issue in our part of the world is one of escalating critical information infrastructure vulnerability. Cyberattacks that target government systems, financial institutions, healthcare networks, and critical energy infrastructure carry the potential to impact national security and economic stability to an unacceptable extent. Shields must be tightened in the face of the critical infrastructure within the chain from cybersecurity defense to continuous network monitoring, threats detection, and neutralization mechanism. The resilience of critical digital infrastructure is thus a major priority in the fight against Cybercrime. The rapid expansion of artificial intelligence and robotics providing an ancillary issue that must be confronted now in the check on cybercrimes. We face a scenario where one engages in a battle in which machine-controlled robots (thanks to artificial intelligence) can identify system vulnerabilities, relay phishing messages, and undertake massive cyber-propelled operations with little or no human intervention. These machines operate with speed and magnitude the traditional cybersecurity systems will find it extremely hard to handle. It is therefore pertinent

[7] UNODC, International Cooperation against Cybercrime.
[8] Pavan Duggal, Cyberlaw: The Indian Perspective (LexisNexis)

 [ISSN 2581-5369]

to develop advanced technologies of cyber defences as well as regulations in order to face the emerging AI-driven cyber-threat to India's response.[9]

VI. LEGAL AND INSTITUTIONAL REFORMS

Centralized investigations may even be carried out by local police divisions at present; however, although private individuals fear reporting offences, they have nowhere to escape when it comes to the case of cybercrime. Hence, ever since the downward trend was witnessed in the table, local investigations appear to have been largely desegregated. This has ensured stronger coordination between different stakeholders and has led to information sharing, such as for criminal intelligence. With the expansion, cyber organisations, including ISPs, cybersecurity organisations, and various related area authorities, have been given additional responsibility. Coordination mechanisms so far developed have helped improve private institutions' corporate work. As such, national authorities were compelled to pass the Computer-Related Offences Act and capabilities.[10] An important role in the prevention of cybercrime is played by initiatives on public awareness and digital literacy. Preparing innovative and engaging computer curricula, advising people about the implications of safe online behavior, maintaining strong security standards in password management, and alertly giving the common people enough information to defend themselves against cybersecurity breaches are among the ways in which an entity can be less vulnerable to cyber threats.

In addition, several measures can be introduced to make cybercrime investigations more efficient. For instance, cybercrime investigations typically entail a substantial amount of digital data from computers, cell phones, cloud storage facilities and online platforms. This makes it all the more necessary to make handling of such evidence in a way that its separation and preservation can be acceptable in the eyes of the law. Especially with large backlogs of general criminal cases that need to be adjudicated and cyberspecific skills at the police and digital forensic labs, no buffer, not to mention confusion and mixed signals hindering prosecution of cybercrime.

Moreover, creating standardized policies for how digital evidence is collected, stored, and analyzed enhances the whole process of enhancing cybercrime evidence integrity and, in a way, helping to boost prosecution when it comes to cybercrime cases. It is a fast and reliable step in an ongoing movement to facilitate the investigations of cybercrime more professionally and has very few setbacks. Moreover, towards achieving the objective of ameliorating cybercrime cases

[9] World Economic Forum, Global Cybersecurity Outlook Report.
[10] National Cyber Coordination Centre, Government of India Reports.

 [ISSN 2581-5369]

imminently, the need for the proliferation of infrastructure.[11]

Furthermore, national leadership must work to establish a resilient national cyber intelligence and monitoring system for cyber threats. Cyber threats are released lightning fast and could target critical infrastructure, the national security sector, or critical financial systems. Developing central cyber intelligence platforms capable of real-time scanning of cyber threats is thus helpful for the Task Forces to detect an early stage of a cyber attack and respond effectively in its suppression. These systems should integrate information from a variety of government departments as well as cybersecurity bodies and international partners to ensure a coordinated response to cyber threats. On the other hand, strengthening the national cyber threat intelligence capabilities is critical to protecting the digital infrastructure of India in the long term cybersecurity.[12]

VII. CONCLUSION

Originally, Cybercrime had widely become one of the most serious challenges of the digital revolution of this century. While India has been busy forging and expanding its digital infrastructure, online services, and e-governance systems, the menace of cybercrime has become even more apparent. The county has taken some legislative steps to address the issue, including those represented in the Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2035, and Bharatiya Nagarik Sureksha Sanhita, 2035, which together outline the legal framework for identifying, investigating, and punishing cybercrimes. The introduction of the Personal Data Protection Act 2023 is indicative of a focus on the protection of privacy and personal data. These laws constitute the central tenets of India's legal framework against cybercrimes. However, practical aspects pose deterrents to the implementation of these legal provisions. The nature of cybercrime is constantly evolving. Criminals use diverse technologies and methods for their offences. The majority of cyber assaults transcend national borders, making their investigation and prosecution a complicated matter. Meanwhile, law enforcement agencies face numerous difficulties in evidence collection and digital forensics, tracing the cyber outlaws and coordinating all interests with foreign authorities. Moreover, during such development, the increased pace of newer technologies, like artificial intelligence, cloud computing, e-commerce, and cryptocurrency, allowed new kinds of cyberattacks for which there is no coverage in the existing laws. Public education is just another critical component in combating cybercrime. The lack of knowledge advices individuals and organizations to become

[11] National Critical Information Infrastructure Protection Centre (NCIIPC), Government of India Reports.
[12] United Nations Office on Drugs and Crime, Comprehensive Study on Cybercrime.

 [ISSN 2581-5369]

victims of cyberattacks. Simple measures such as using strong passcodes, abstaining from doubtful web links, ensuring the safety of personal data, or lodging a report on cyber incidents can diminish chances of falling victim to cybercrime. A collaborative alliance among government departments working together with educational institutions and private organizations must respond to increasing public knowledge on cyber and digital literacy. In conclusion, India has established a technology-oriented law on cybercrime, but there is a dire need for an enhanced framework to meet the threats and realization of its changes in pace and form and to identify such society-facilitating measures. Updating these laws, improving institutional abilities, enhancing international cooperation, and promoting the public's awareness are essential to combating cybercrime effectively in the foreseeable future. A balanced outlook supporting both digital security and individual liberties will not only provide a safer and a secure cyberspace for one and all but will equally be the foundation of deep-rooted nineteenth-century moral and social values.

*****

 [ISSN 2581-5369]