Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume: 3 Issue:1
July 2025
Impact Factor: 11.9
Subject: Law

A Critical Evaluation of the New Criminal Law to Address Emerging Digital and Cybercrime Threats

Dr. Ramesh Kumar Singh
Assistant Professor
Veer Kunwar Singh University, Ara Bihar
Posted at Maharaja Law College, Ara

Abstract

The digital growth in India has been characterised by a sudden surge in cybercrime, viz. identify theft and phishing, cyber-stalking, data breach, and abuse of new technologies like AI and blockchains, among others. It was only recently when the nation used to be governed by colonial laws, such as Indian Penal Code (I.P.C), and did little employment and applied little to the Information Technology Act, 2000, which were practically incapable of protecting the nation against the magnitude and severity of current cyber-attacks. This paper presents a critical analysis of the recently promulgated Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS), and Bharatiya Sakshya Adhiniyam (BSA) so as to analyze its relevance and suitability in dealing with digital and cybercrime. The research establishes major developments through the doctrinal analysis and comparative legal review, including the identification of new crimes of digital nature and electronic evidence, e-FIR, and procedural reforms. It also identifies lingering gaps such as deficiency in definitions, and existence of cross-border investigation protocols, and issues bordering on privacy and surveillance. The researchers argue that although the new institutional architecture should be taken as a major leap, its effectiveness will hinge on strong institutional capacities, effective digital infrastructure and law-making flexibility. Legal enforcement through training, forensic readiness, and clarity with laws must be strategic factors that will ensure a safe digital legal system.

Keywords: Cybercrime, Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita, Bharatiya Sakshya Adhiniyam, Digital Evidence, Cyber Law Reform.

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume: 3 Issue:1
July 2025
Impact Factor: 11.9
Subject: Law

1. INTRODUCTION

Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS) and Bharatiya Sakshya Adhiniyam (BSA) have opened some greener pasture in the development of criminal justice system in India. These are stern attempts to modernize the criminal justice system of the country and liberate it of the colonialism. To improve accessibility, efficiency, and increased citizen focus of justice, structural changes to the system such as digital integration, limited time to act, codification of new offences and more effective accountability of people have been proposed in the new framework (Amoo et al., 2024). Similarly, the reforms of the doctrine namely the redefinition of sedition, formal acknowledgement of organised crimes, and increased emphasis on victim involvement reveal the fact that people are awakening to how things are like today in the political, social and legal sphere (Giannakoula et al., 2020).

The last two decades witnessed tremendous digital growth in India in terms of increased number of people using the internet, increased number of people receiving mobile connection, digital banking, and e-governance. These developments have become easier ways of getting services and communicating with other people, and on the other side, this has become riskier. Crime has evolved over a time, now it is in cyberspace. Phishing, identity theft, online financial frauds, data breaches, ransomware attacks, cyberstalking, digital defamation are the cybercrimes that are fast to be on the rise in India. According to the National Crime Records Bureau (NCRB), the number of cybercrimes registered in India increased by over 60 percent between 2018-2022. This increase demonstrates the necessity of modern and effective legal framework that will be capable of coping with such complex and cross-border nature of cyber-attacks (Batrachenko et al., 2024).

India had predominantly the Indian Penal Code, 1860 (IPC) and the Information Technology Act, 2000 (IT Act) that were used to address the cybercrimes. However, the IPC was composed before the internet had been widely adopted, and so it does not explicitly discuss cyber-enabled crimes. This implies that prosecutors are usually forced to utilize outdated or unsuitable legislations. The IT Act was a legislation which covered the electronic crimes but it was really more of rules rather than a crime and it did not even carry much land (Afaq et al., 2023). A lot of crimes, such as cyberterrorism, data manipulation, and distributing deepfakes, also lack proper definitions and sufficient punishment, along with complex digital financial frauds. Even

ISSN: 2320-3714
Volume: 3 Issue:1
July 2025
Impact Factor: 11.9
Subject: Law

the criminal procedure code, 1973(CrPC) lacked any methodologies in addressing digital evidence, interstate investigation, or real-time requirements in cyberforensic situations.

The Indian Parliament passed three new laws in 2023 to get around these problems:

- The Bharatiya Nyaya Sanhita (BNS), 2023, takes the place of the IPC.
- The Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, takes the place of the CrPC.
- The Bharatiya Sakshya Adhiniyam (BSA), 2023, takes the place of the Indian Evidence Act, 1872.

The changes will aim at ensuring that the criminal justice system becomes less colonial and aligned with our current life, especially the digital era. As an example, the BNS has laws against cyber fraud, identity theft, and data breaches. With the BNSS you can submit e-FIRs, conduct remote trials, and conduct investigations with the help of electronic tools. According to the official statement of the BSA, electronic evidence can be presented in the form of electronic records, i.e., electronic papers on clouds, blockchain-based authentication, and metadata.

Cybercrime continuously evolves and becomes more complex, so we should pay much attention to the new laws that should protect us against present and potential online threats. This paper will seek to examine the advantages and disadvantages of the new legislations on cybercrimes and implications in the real life.

1.1.Objectives

The objectives are:

- To examine the particular digital and cyber-specified sections of the new criminal laws. Determining whether these provisions fill the missing link of previous laws
- To look at whether law enforcement, courts and forensic institutions are prepared to use these laws
- To recommend the modification of legislation and policies so that the reaction of India to cybercrime can be more powerful.

1.2.Methodology and scope

The study is of a doctrinal method and analytical. It is done through screening of the key legislative documents (BNS, BNSS, BSA), its cross-examination to the IPC, CrPC and IT Act,

ISSN: 2320-3714
Volume: 3 Issue:1
July 2025
Impact Factor: 11.9
Subject: Law

and relevant judicial opinions. We also turn to the secondary sources such as government sources, cybercrime statistics, articles by scholars, and comments by experts. The study examines regulations that deal exclusively on cybercrime, electronic evidence, methods of investigation and technological capaciti es. The gist of the paper is to examine the evolution of laws in India. It also throws into comparison that of India in terms of the best practices followed anywhere in the world.

2. PROVISIONS IN THE NEW CRIMINAL LAW FRAMEWORK RELATED TO CYBERCRIME

The new criminal law structure consists of the Bharatiya Nagarik Suraksha Sanhita (BNSS), Bharatiya Nyaya Sanhita (BNS), and Bharatiya Sakshya Adhiniyam (BSA). It is a significant amendment in the law, which will modernize the criminal justice system in India (Jayawibawa, 2024). Among the biggest purposed of such changes is to cope with the growing complexity as well as the growing sheer size of cybercrime. Colonial-era laws could never be able to cope with the same satisfactorily. These new laws do not only alter what constitutes a crime to be more digital but this also alters the way evidence is gathered and how cases are processed to accommodate the new-fangled world of cybercrimes (Buçaj & Idrizaj, 2025).

2.1.Bharatiya Nyaya Sanhita (BNS): Substantive Cybercrime Provisions

The BNS, 2023, replaces the IPC and gives an addition to some new cybercrimes that are specifically outlined in sections. It is making the crimes which employ digital technologies, more obvious and more turbo controlled.

Table 1: Key Cyber-Related Offences in Bharatiya Nyaya Sanhita

Provision	Offence	New Additions / Changes	Remarks
Section 73	Cheating by personation using computer resources	Inclusion of identity theft through electronic means	Previously vague under IPC Sec 416
Section 107	Cyberstalking	Recognized as a distinct offence involving digital harassment	Not explicitly defined in IPC

ISSN: 2320-3714
Volume: 3 Issue:1
July 2025
Impact Factor: 11.9
Subject: Law

Section 66	Fraudulent digital transactions	Covers financial fraud through UPI, net banking, etc.	Addressed previously only under IT Act
Section 336	Publication of obscene material in electronic form	Explicitly includes social media and messaging platforms	Builds upon Sec 67 of IT Act, 2000
Section 113	Voyeurism and morphing using AI/deepfake tools	Modern inclusion addressing image-based sexual abuse	Not covered previously

The new functions are designed to ward off the vast majority of online threats, such as phishing, revenge porn, impersonation on the digital platforms, and financial fraud (Oreku & Mtenzi, 2017).

2.2.Bharatiya Nagarik Suraksha Sanhita (BNSS): Procedural Innovations

The BNSS, 2023 that is substitutable to the CrPC makes several adjustments to how things should be done to assist in managing cybercrimes in real-time. It realizes the value of speed, the incorporation of technologies and partnership in cybercrime investigations (Atrey, 2023).

Table 2: Procedural Reforms for Cybercrime Investigation in BNSS

Provision	**Description**	**Improvement Over CrPC**
Section 173(3)	E-FIR can be filed remotely without jurisdictional limitation	FIR filing was restricted to physical mode
Section 176(3)	Forensic analysis is mandatory for crimes with punishment ≥ 7 years	Forensics were discretionary and delayed
Section 193	Trials can be conducted via video conferencing	Remote trials lacked legal backing

ISSN: 2320-3714
Volume: 3 Issue:1
July 2025
Impact Factor: 11.9
Subject: Law

Section 195	Provision for protection of digital witnesses and whistleblowers	Absent in CrPC
Section 105	Use of electronic summons, arrest warrants through secure digital transmission	Previously required physical service of notice

This is to help in streamlining the ongoing digital investigations and eliminate reliance on physical records as well as enhancing cooperation among agencies through the electronic mediums.

2.3.Bharatiya Sakshya Adhiniyam (BSA): Evidentiary Strength for Digital Data

The Bharatiya Sakshya Adhiniyam, 2023 reformulates the rules of evidence in view of the digitalization of communications and trade. It focuses on admissibility, authentication and integrity of electronic evidence.

Table 3: Evidentiary Changes in Bharatiya Sakshya Adhiniyam (BSA)

Provision	**Nature of Evidence Recognized**	**Improvement Over Evidence Act, 1872**
Section 63	Admissibility of electronic and digital records	Replaces outdated Sec 65B with simplified procedures
Section 65	Recognition of cloud storage, encrypted files, metadata	IT Act didn't cover secure cloud/remote servers
Section 71	Blockchain, biometric, and GPS data admissible	No mention in previous evidence laws
Section 76	Digital signature verification and e-record certification	More structured than ad hoc digital certificate rules
Section 80	Presumption of authenticity for government digital records	Encourages use of e-governance documents in trials

ISSN: 2320-3714
Volume: 3 Issue:1
July 2025
Impact Factor: 11.9
Subject: Law

The BSA brings the evidence law of India in line with international best practices enabling easier prosecution of the cases of digital crime and high integrity of data during the trial process (Pandey et al., 2023).

2.4.Comparison with Previous Legal Frameworks

In order to get the significance of the level of progress, it is imperative to contrast these new rules to their earlier versions, i.e., the IPC, CrPC, Evidence Act, and the IT Act (Martin & Rice, 2011).

Table 4: Comparative View of Old vs. New Legal Provisions

Aspect	**Old Framework (IPC/CrPC/IEA/IT Act)**	**New Framework (BNS/BNSS/BSA)**
Cybercrime definitions	Scattered or missing; vague references	Specific, updated, and technology-focused
FIR and jurisdiction	FIR limited by local police jurisdiction	E-FIR and zero FIR recognized
Digital evidence	Relied on Section 65B (Evidence Act), often misapplied	Clear definitions and admissibility in BSA
Trial process	Only physical appearances allowed	Legalized remote trials via video conferencing
Forensic and tech support	No mandatory digital forensics	Compulsory in serious offences (≥7 years)
Modern tech recognition	No mention of blockchain, AI, cloud data	Included in evidentiary and investigative provisions

3. CRITICAL EVALUATION OF THE EFFECTIVENESS AND CHALLENGES

The new criminal law framework in India includes the Bharatiya Nyaya Sanhita (BNS), the Bharatiya Nagarik Suraksha Sanhita (BNSS) and the Bharatiya Sakshya Adhiniyam (BSA).

ISSN: 2320-3714
Volume: 3 Issue:1
July 2025
Impact Factor: 11.9
Subject: Law

This will be a massive milestone into the modernisation of the law to address new issues, in particular in the digital realm. Though the revisions attempt to seal old loopholes in the law concerning cybercrime, their effectiveness in practice is determined by several factors. This section critically examines the strength and weaknesses of the new rules (Sumadinata, 2023).

3.1.Strengths of the new provisions

The only wonderful aspect of the new criminal law system is that it attempts to bring the legal system of India closer to the way in which things would be since everything is online. The Indian Evidence Law (Bharatiya Sakshya Adhiniyam; BSA) clearly indicates that electronic data (such as emails, cloud data, blockchain data, and GPS data) may be presented as evidence. It is a major improvement of the old Indian Evidence Act where Section 65B was utilized and regularly misunderstood or applied differently before the court (Yar & Steinmetz, 2023).

Procedural improvement is also made by the BNSS in terms of e-FIR, video conference service (remotely conducted trials) and compulsory forensic examination in serious cases. The aim of these advances is that investigations and trial can be done more rapidly, which is extremely significant in cyber related cases where digital evidence must be preserved as rapidly as possible.

The BNS, in turn, specifically spells out the crimes of new age, such as cyberstalking, digital identity theft, or harassment through deepfakes, which either were not well outlined or were absent at all in the IPC. The law needs this understanding so that it can address in an efficient mode the ever-changing nature of digital crimes.

3.2.Gaps and ambiguities

There are still some things that remain unclear or absent even with the new laws already in motion. Among the key issues, one can distinguish the fact that digital crimes are complicated and constantly evolving with no clear definitions. As an example, identity theft and cyber fraud are crimes that are familiar to us, and crimes such as those involving cryptocurrency, artificial intelligence-created fake data, or illicit trafficking in the dark net are not yet clearly defined.

The jurisdiction issues are not resolved yet. Most cyber-crimes occur in multiple states, the BNSS has no guidelines on how to collaborate across the borders, assist one another within the

ISSN: 2320-3714
Volume: 3 Issue:1
July 2025
Impact Factor: 11.9
Subject: Law

bounds of the law, or how to access data internationally, which are all very critical when it comes to investigating cyber-crimes (Kulshrestha et al., 2022).

Additionally, some standards of procedure still rely on out-dated paradigms of investigation, including reliance heavily upon hard-copy materials and face-to-face depositions, which cannot be relied upon in a cybercrime investigation or, where relied upon, may be of limited value or use.

3.3.Concerns related to surveillance, privacy, and misuse of digital evidence

The BSA helps to use electronic evidence in court, but it does not contribute much to privacy and data protection. The criminal laws do not seem to have a particular regulation regarding the surveillance techniques and this is a cause of concern among the people who fear that the law enforcement authorities can use their mandate erroneously. As an example, allowing content of WhatsApp messages, logs of calls or cloud data to be presented as evidence without any strict data protection laws may contravene Article 21 of India Constitution which is the right to privacy (Justice K.S. Puttaswamy v. India Union, 2017). The expanded scope of monitoring, however, in the absence of robust court scrutiny and warrants, would result in profiling, unlawful search and unlawful incrimination.

3.4.Institutional and infrastructure limitations

One of the largest issues of the Indian criminal justice system that will complicate the execution of these reforms is its institutional inability. The rules are different and so is the supporting infrastructure.

Cyber forensic labs in India are lacking significantly including in the rural parts or the Tier-2 cities. The majority of the police officers have not yet learned how to effectively handle crimes that are committed on the Internet and how to trace the digital procedures of the new laws (Cassidy et al., 2024).

Judges and other court officials also require workshops that could assist them to remember and analyze the digital evidence, particularly complicated cases that involve AI or blockchain data. The interstate and the interpolice digital divide is also a vast issue. Even an access to elementary

ISSN: 2320-3714
Volume: 3 Issue:1
July 2025
Impact Factor: 11.9
Subject: Law

internet or digitally organized records and secure data storing locations are a problem in most police outlets (Nosál, 2023).

4. CONCLUSION AND RECOMMENDATIONS

The principal findings of the current research will prove that the new legislation has helped the judicial system become more robust, as such crimes as cyberstalking, identity theft, and online fraud are clear in the law, and such processes as e-FIRs and trials performed remotely are faster. The Bharatiya Sakshya Adhiniyam also takes the huge leap towards accepting that digital evidence such as cloud data, blockchain entries, and GPS tracks can be presented in the court. Nevertheless, there are still a few blank spots, as inexact definitions of the new phenomena of cyber threats, such as deepfake manipulation, crypto-related fraud, and misinformation by AI-powered media. Some of these barriers imposed by the institutions have to do with limited cyber forensic capacity, ineffective training among the police and the absence of the digital infrastructure to implement these laws as well.

It Concluding on the basis of the results, several policy recommendations are proposed. One, the police units as well as the courts should devise a set of useful guidelines and operating procedures in regard to the investigations and collection of information relating to cybercrime as well as information in a digital form. Secondly, there must be a centralised digital crime coordination team to assist in the investigations that cross national borders and coordinate with other states. Third, police, prosecutors and judges will need to undergo the necessary courses in cyber forensics, privacy laws in information communication technology and safeguards when using electronic surveillance to ensure they are conversant with the application of the new laws.

The amendments of the law that will be made in the future need to be aimed at the clarification of the definition and the scope of the new crimes. These crimes involve those which occur at the dark web, cryptocurrency fraud, the misuse of artificial intelligence, and liability breach regarding data. We also require a complete Data Protection justice, which should accompany the criminal justice system and protect the rights of people in a world where Surveillance is gradually becoming a rampant activity. It should also work out on its ability to keep up with the rapid changes in the aspect of technology by updating of procedural procedures and handling of evidence.

ISSN: 2320-3714
Volume: 3 Issue:1
July 2025
Impact Factor: 11.9
Subject: Law

It is the flexibility of the state to transform which will make any legislative fabric work so as to halt cybercrime. The Indian code has to look at the implementation of the adaptive law making whereby laws, rules and enforcement mechanisms are re-written every now and then in response to digital trends and stakeholders. As the world is fast paced with technology that outstrips the law, the success of the law will be decided on its adaptability in responding, clarity and flexibility of its institutions. By integrating foresight in law with practical capacity-building, India can demonstrate the way of handling the digital issues, respect to the rule of law, and protect the fundamental rights.

REFERENCES

1. Amoo, O. O., Atadoga, A., Abrahams, T. O., Farayola, O. A., Osasona, F., & Ayinla, B. S. (2024). The legal landscape of cybercrime: A review of contemporary issues in the criminal justice system. *World Journal of Advanced Research and Reviews*, *21*(2), 205-217.
2. Atrey, I. (2023). Cybercrime and its Legal Implications: Analysing the challenges and Legal frameworks surrounding Cybercrime, including issues related to Jurisdiction, Privacy, and Digital Evidence. *International Journal of Research and Analytical Reviews*.
3. Batrachenko, T., Lehan, I., Kuchmenko, V., Kovalchuk, V., & Mazurenko, O. (2024). Cybercrime in the context of the digital age: analysis of threats, legal challenges and strategies. *Multidisciplinary Science Journal*, *6*.
4. Buçaj, E., & Idrizaj, K. (2025). The need for cybercrime regulation on a global scale by the international law and cyber convention. *Multidisciplinary Reviews*, *8*(1), 2025024-2025024.
5. Cassidy, A. A. T. J., Fuad, A., & Shofy, M. U. A. A. (2024). Emerging Trends and Challenges in Digital Crime: A Study of Cyber Criminal Tactics and Countermeasures. *TechComp Innovations: Journal of Computer Science and Technology*, *1*(1), 38-45.
6. Kulshrestha, P., Gautam, R., & Singh, A. (Eds.). (2022). *Cyber Crime, Regulation and Security: Contemporary Issues and Challenges*. Libertatem Media Private Limited.

ISSN: 2320-3714
Volume: 3 Issue:1
July 2025
Impact Factor: 11.9
Subject: Law

7. Nosál, J. (2023). Crime in the digital age: A new frontier. In *The Implications of Emerging Technologies in the Euro-Atlantic Space: Views from the Younger Generation Leaders Network* (pp. 177-193). Cham: Springer International Publishing.
8. Oreku, G. S., & Mtenzi, F. J. (2017). Cybercrime: Concerns, challenges and opportunities. *Information Fusion for Cyber-Security Analytics*, 129-153.
9. Pandey, A. K. (2023). The role of technology in modernizing criminal law: Addressing cybercrime and digital evidence.
10. Sumadinata, W. S. (2023). Cybercrime and global security threats: A challenge in international law. *Russian Law Journal*, *11*(3), 438-444.
11. Giannakoula, A., Lima, D., & Kaiafa-Gbandi, M. (2020). Combating crime in the digital age: a critical review of EU information systems in the area of freedom, security and justice in the post-interoperability era: challenges for criminal law and personal data protection. *Brill Research Perspectives in Transnational Crime*, *2*(4), 1-97.
12. Afaq, S. A., Husain, M. S., Bello, A., & Sadia, H. (2023). A critical analysis of cyber threats and their global impact. In *Computational Intelligent Security in Wireless Communications* (pp. 201-220). CRC Press.
13. Martin, N., & Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security*, *30*(8), 803-814.
14. Yar, M., & Steinmetz, K. F. (2023). Cybercrime and society.
15. Jayawibawa, M. H. (2024). UNRAVELING JUSTICE: THE EVOLVING LANDSCAPE OF CRIMINAL LAW IN THE MODERN ERA: UNRAVELING JUSTICE: THE EVOLVING LANDSCAPE OF CRIMINAL LAW IN THE MODERN ERA. *PENA LAW: International Journal of Law*, *2*(2).

Airo International Journal
Peer-Reviewed
Multidisciplinary

ISSN: 2320-3714
Volume: 3 Issue:1
July 2025
Impact Factor: 11.9
Subject: Law

Author's Declaration

I as an author of the above research paper/article, here by, declare that the content of this paper is prepared by me and if any person having copyright issue or patent or anything otherwise related to the content, I shall always be legally responsible for any issue. For the reason of invisibility of my research paper on the website /amendments /updates, I have resubmitted my paper for publication on the same date. If any data or information given by me is not correct, I shall always be legally responsible. With my whole responsibility legally and formally have intimated the publisher (Publisher) that my paper has been checked by my guide (if any) or expert to make it sure that paper is technically right and there is no unaccepted plagiarism and hentriacontane is genuinely mine. If any issue arises related to Plagiarism/ Guide Name/ Educational Qualification /Designation /Address of my university/ college/institution/ Structure or Formatting/ Resubmission /Submission /Copyright /Patent /Submission for any higher degree or Job/Primary Data/Secondary Data Issues. I will be solely/entirely responsible for any legal issues. I have been informed that the most of the data from the website is invisible or shuffled or vanished from the database due to some technical fault or hacking and therefore the process of resubmission is there for the scholars/students who finds trouble in getting their paper on the website. At the time of resubmission of my paper I take all the legal and formal responsibilities, If I hide or do not submit the copy of my original documents (Andhra/Driving License/Any Identity Proof and Photo) in spite of demand from the publisher then my paper maybe rejected or removed from the website anytime and may not be consider for verification. I accept the fact that as the content of this paper and the resubmission legal responsibilities and reasons are only mine then the Publisher (Airo International Journal/Airo National Research Journal) is never responsible. I also declare that if publisher finds Any complication or error or anything hidden or implemented otherwise, my paper maybe removed from the website or the watermark of remark/actuality maybe mentioned on my paper. Even if anything is found illegal publisher may also take legal action against me.

Dr. Ramesh Kumar Singh

*****