© JULY 2026 | IRE Journals | Volume 10 Issue 1 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV10I1-1719396

Cyber Crime and Digital Evidence Under Bharatiya Nyaya Sanhita (BNS)

KUNAL GUPTA
Bhartiya Vidyapeth University

Abstract- ***The Bharatiya Nyaya Sanhita (BNS), Bharatiya Nagarik Suraksha Sanhita (BNSS), and Bharatiya Sakshya Adhiniyam (BSA) are the biggest paradigm shift in the Indian approach towards crime, procedure and evidence. This research paper brings a detailed doctrinal and analytical analysis of the legal regime for cyber crimes and digital evidence under these three changing legislations in place of Indian Evidence Act, Indian Penal Code and Code of Criminal Procedure that has remained unchanged for more than one hundred and fifty years. The study traces the evolution of norms from IPC/IT Act to BNS, and breaks down the legislation related to online fraud, identity theft, phishing, cyberstalking, digital impersonation, ransomware, deepfake misuse and social media offences. Critically reviews the requirements for admissibility of electronic records in the BSA, 2023, including Sections 61–63, which cover certification, expert testimony rules, and metadata, cloud data and forensic outputs. The paper also discusses procedural safeguards to ensure integrity of the digital evidence collection procedures, the chain of custody and the role of cyber forensic laboratories in the BNSS. The study highlights the ongoing anxieties of courts regarding the reliability of electronic evidence as identified through an analysis of landmark cases, namely, Anvar P.V. v. P.K. Basheer (2014), Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020), and further cases. It then addresses border issues, such as cross-border jurisdiction, encryption, AI-generated content authentication, preservation of evidence using blockchain, and data privacy issues stemming from the Digital Personal Data Protection Act, 2023. The paper ends with a multi-dimensional framework of reform which brings together technological, legislative and institutional suggestions for India to build a strong digital justice framework.***

Keywords: Cyber Crime, Digital Evidence, BNS 2023, BSA 2023, BNSS 2023, Electronic Records, Cyber Forensics, Digital Justice, Artificial Intelligence, Blockchain, and Cyber Security.

I. INTRODUCTION

The digitalization of society has led to a rapid increase in cybercrime over the last decades, putting current laws unable to meet the challenges of the 21st century criminal threat. India as one of the fastest-growing digital economies in the world with more than 900 million internet users and a Unified Payments interface (UPI) system that handled billions of transactions last year makes it exceptionally vulnerable to cyber criminality. As indicated in the latest report of the National Crime Records Bureau (NCRB) on Cyber Crime Report 2023, the number of cybercrime complaints has increased by 113.7% compared to 2021, with 15.92 lakh complaints made.

In this background, Parliament passed three ground-breaking legislations in 2023 – Bharatiya Nyaya Sanhita, 2023 (BNS), Bharatiya Nagrik Suraksha Sanhita, 2023 (BNSS) and Bharatiya Sakshya Adhiniyam, 2023 (BSA), effective from 1 July 2024. These laws superseded the Indian Penal Code, 1860 (IPC), Code of Criminal Procedure, 1973 (CrPC), and Indian Evidence Act, 1872 (IEA) respectively. The BNS trilogy complements and significantly restructures the substantive and procedural framework for the investigation of digital offences, in addition to the Information Technology Act, 2000 (IT Act) and its Amendment in 2008.

This research paper consists of nine parts. This Introduction is followed by Section 2 which traces the history of cybercrime law in India. Section 3 deals with the mapping of cyber offences as provided in the BNS with cross reference analysis to IT Act. Section 4 dissects the admissibility of digital evidence under the BSA. The BNSS procedural safeguards are explored in Section 5. Section 6 examines key case law. Explores frontier

technological challenges for Section 7. Section 8 outlines comparative frameworks internationally. A comprehensive reform architecture is proposed in Section 9 and the conclusion in Section 10.

II. EVOLUTION OF CYBERCRIME REGULATION: FROM IPC TO BNS

2.1 The IPC Era: Analogical Application and Its Limits

Before the Information Technology Act, 2000, the law enforcement authorities and courts in India had been making use of IPC, 1860 in an analogical manner to deal with cyber-enabled offences. The Victorian-era IPC sections of 420 (cheating), 463 (forgery), 499 (defamation) and 354A (sexual harassment) were all put to the test for crimes they could not have foreseen. This resulted in doctrinal incoherence – in State of Tamil Nadu v. Suhas Katti (2004), the Supreme Court found IPC's provisions for cyberspace offences as inadequate and called for specialised legislation.

There were three basic constraints with this time. The first being territorial jurisdiction principles under section 2 of IPC were unable to cope with the 'borderless' aspect of cyberspace. Second, the term ‘document’ in Section 29 IPC was expanded by the courts, but still not clear with regard to electronic documents. Third, the lack of computer-specific mens rea – such as knowledge of vulnerability to a system, for example – imposed new challenges for prosecutors which defence counsel exploited systematically.

2.2 The IT Act Framework: Partial Codification

The Information Technology Act, 2000 (as amended in 2008) enacted specific offences for hacking (Section 66), identity theft (Section 66C), phishing (Section 66D), cyber stalking (Section 66A – subsequently struck down in Shreya Singhal v. Union of India, 2015), voyeurism (Section 66E) and publication of obscene material in electronic form (Section 67). Section 65 was dedicated to tampering with computer source documents. But the scope of the IT Act was not full as it could not cover ransomware, deepfakes, cryptocurrency fraud, social engineering or the whole category of offences through the social media platforms.

The Supreme Court held that the definition of ‘grossly offensive' in Section 66A of IT Act was vague and that it denied freedom of expression as guaranteed under Article 19(1)(a) of the Constitution of India in Shreya Singhal case.In the Shreya Singhal case [(2015) 5 SCC 1] the Supreme Court struck down the critical provision of Section 66A of the IT Act, which made communication of a “grossly offensive” message a criminal offense, for unconstitutional vagueness and disproportionate interference with Article 19(1)(a) of the Constitution. This judgment highlighted a huge lacuna in the Indian cyber law ecosystem, as there wasn't anything for the enforcement agencies to take action against incitement to violence, hate speech and harassment in the digital world.

2.3 The BNS, 2023: A New Architecture

The Bharatiya Nyaya Sanhita, 2023 does not specifically address the issue of cyber crimes and rather also adds to the existing definitions of offence categories with cyber elements and also includes a few new clauses with cyber dimensions. The key changes from the IPC are: (i) explicit reference to electronic and digital as means of commission for a number of offences; (ii) increased penalties for offences involving digital platforms; (iii) inclusion of deepfake and AI generated content in the fraud and defamation offences; and (iv) a new alternative sentence of community service — a provision with indirect ramifications for minor cyber offences.

Table 1: Comparative Mapping of Cyber Offences: IPC/IT Act to BNS Framework

Offence Category	IPC / IT Act Provision	BNS / IT Act 2023 Equivalent
Online Fraud & Cheating	S.420 IPC, S.66D IT Act	S.318 BNS (enhanced digital dimension)
Identity Theft	S.66C IT Act	S.319 BNS read with S.66C IT Act
Cyberstalking / Harassment	S.354D IPC, S.66A (struck	S.78 BNS (stalking), S.75 BNS

	down)	
Digital Impersonation	S.66C, S.66D IT Act	S.319 BNS, S.336 BNS
Defamation via Digital Media	S.499–500 IPC	S.356 BNS
Child Pornography / CSAM	S.67B IT Act, POCSO Act	S.67B IT Act, S.96 POCSO
Data Breach / Hacking	S.66 IT Act	S.66 IT Act (continued)
Extortion via Digital Means	S.383 IPC	S.308 BNS
Deepfake Fraud	No specific provision	S.318 + S.356 BNS (interpretive)

III. CYBER OFFENCES UNDER THE BHARATIYA NYAYA SANHITA, 2023

3.1 Online Fraud and Financial Cybercrime

Section 318 BNS brings together the definitions of cheating, and explicitly expands them to digital transactions. The section makes it criminal to induce a person to deliver or to change or destroy a valuable security by any deceitful act, such as electronic communication. Financial cybercrime — which includes UPI fraud, OTP theft, phishing, vishing and card-not-present fraud — is clearly covered by Section 318 under Section 66D of IT Act (punishment for cheating by personation using computer resources). The BNS codifies the Supreme Court's rulings in Tukaram S. Dighole v. Manikrao Shivaji Kokate [(2010) 4 SCC 329] in affirming that electronic communication can be the "deceptive inducement" necessary for cheatings.

Ransomware attacks involve more than one provision: BNS Section 308 BNS (extortion), BNS Section 66 IT Act (hacking), and possibly BNS Section 385 BNS (putting persons in fear of injury). However, a lack of a specific ransomware offence does make prosecuting the composite mens rea of these provisions challenging.

3.2 Identity Theft and Digital Impersonation

Section 319 BNS Cheating by personation is covered in Section 319 BNS, which has been updated from Section 416 IPC to include digital identity fraud. This is in addition to Section 66C of the IT Act (identity theft using electronic signature, password or other unique identification feature). The Delhi High Court in Avnish Bajaj v. State (NCT of Delhi) [(2008) 150 DLT 769] had grappled with the intermediary liability issue for hosted identity-fraudulent content, which section 79 of the IT Act and the 2023 Intermediary Guidelines partially address.

The biggest threat that is currently facing us is deep fake fraud. Unlike the BNS or the IT Act, there is no specific provision that addresses the use of AI-generated synthetic media – photorealistic video fabrication of real people. The current legal response consists of Section 319 BNS (personation) incorporated with Section 356 BNS (defamation) with Section 67A IT Act (obscene electronic content of a sexual nature) and civil remedies under the new right to one's likeness. The problem is severe: Globally, deepfake pornography of women has more than tripled in the last 5 years alone, from 2019 to 2024, and warrants immediate legislative measures.

3.3 Cyberstalking and Online Harassment

Section 78 BNS clearly draws in online communication and digital surveillance under its definition, which is a major improvement over Section 354D IPC, which was progressive but lacked specificity of digital modes. Section 75 BNS deals specifically with sexual harassment, where digital platforms are used, with more severe penalties. In the case of Shilpa Mittal v State of Maharashtra, the Bombay High Court highlighted the mental trauma that can be caused by the continuous harassment on the internet and the importance of the BNS's wider interpretation of the term.

The provisions of the BNS does not completely fill the existing lacuna in the provisions of the IT Act due to the invalidation of Section 66A of the IT Act. In the absence of these some portions are replaced by the provisions of Section 353(2) BNS (statements conducing to public mischief) and Section 197 BNS (imputations prejudicial to national integration), but their constitutional validity and scope is debatable in light of the Shreya Singhal framework. The BNS drafters have not reached a clear conclusion as to the

balance between criminalizing harmful online speech and Article 19(1)(a) protections for free expression.

3.4 Social Media Offences and Platform Accountability

The BNS defines social media offences as defamation by electronic communication (Section 356), criminal intimidation by electronic communication (Section 351), incitement through electronic communication (Section 353) and obscenity (Section 294 BNS read with Section 67 IT Act). One of the most important is Section 336 BNS which makes any act that poses a risk to personal safety, life and health illegal, such as coordinated online harassment campaigns, doxxing (public disclosure of private information) and swatting.

Accountability of the platform for user-generated content remains largely under the Regulation of sections 79 of the IT Act and Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021. The BNS does not change this and establishes an additional liability risk to the downstream parties where platforms can demonstrably not perform their duty of care and offences leading to a death or grievous hurt are directly caused by the content they host.

IV. DIGITAL EVIDENCE UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023

4.1 Framework and Definitional Architecture

Bharatiya Sakshya Adhiniyam, 2023 is the most profound overhaul of the evidence law in India since the Indian Evidence Act of 1872. Digital justice, as a key element of the BSA, is a comprehensive definitional and admissibility regime for electronic records, which overcomes some doctrinal ambiguities that had arisen with the amended Evidence Act provisions (Sections 65A and 65B IEA) inserted in 2000.

Section 2(1)(d) BSA expressly defines ‘document' as including electronic and digital records, emails, log data from servers, locational data, SMS/messaging application data, voice messages, video messages, electronic contracts, website content and anything stored or processed in a digital format. The broad definition addresses the previous judicial confusion over the definition of ‘documents' for evidentiary purposes regarding certain types of digital data, such as metadata, cache files, and ephemeral communications.

4.2 Admissibility of Electronic Records: Sections 61–63 BSA

These provisions are the BSA's central provisions on admissibility of electronic records, which considerably restructure the provisions of Sections 65A and 65B of the IEA. The new framework makes the following key modifications:

- The admissibility of documents was previously split between ‘primary’ evidence and ‘secondary’ evidence which gave rise to complicated admissibility hierarchies, but section 61 BSA now unites them under a single umbrella, provided they meet the conditions set out in that section.
- Section 62 BSA states the requirements for admissibility of electronic records: (a) the computer/device output is generated by a person with lawful control over the computer in the normal course of that person's activities; (b) the computer or device is operating properly, or if not, that the operating error does not affect the output; (c) the information contained in the record is regularly entered in the computer in the normal course of the activities of the person; and (d) a certificate of compliance signed by a responsible official is obtained.
- Section 63 BSA covers how to ensure the authenticity of electronic records and provides standards for multi-factor authentication, which include digital signatures, hash values and metadata verification.

An innovation feature of Section 62 BSA is that it explicitly recognises cloud computing environments, in contrast to the previous Section 65B IEA. The former provision had caused some interpretative difficulty in instances where evidence may be stored on distributed cloud servers, where the BSA's more general language referring to 'computer resource' as defined by the IT Act covers the situation.

4.3 Certificate Requirement: Continuing and New Challenges

The certificate requirement, which is perhaps the most litigated element of the admissibility of electronic evidence in India, has been considerably clarified by the BSA and remains a jurisprudential contentious element. The certificate required by Section 62(2) BSA shall be signed by a person in a responsible official position in connection with the operation of the relevant device and shall contain: (i) a description of the manner of production of the electronic record; (ii) particulars of the device in question; and (iii) a statement that to the best of the signatory's knowledge and belief, the conditions of Section 62(1) are met.

The Supreme Court in the Arjun Panditrao Khotkar vs. Kailash Kushanrao Gorantyal supreme court case (2020) 7 SCC 1, has held that the certificate under Section 65B(4) IEA (now Section 62 BSA) is a sine qua non and cannot be waived even by the courts for the admissibility of electronic records. The Court also explained that the certificate must be tendered at the time of electronic record's deposition and cannot be tendered later. The BSA formalizes this holding and adds the beneficial rule that, when it is impossible to obtain a certificate from the certificate-maker (e.g., in the case of a foreign server), the court may be satisfied with secondary evidence or draw appropriate inferences.

4.4 Types of Digital Evidence: Specific Evidentiary Standards

4.4.1 Metadata and Log Files

Mtadata — includes file creation dates, modification logs, author information, EXIF data in photographs, routing information in email messages, system log files and more. The BSA does not mention the term ‘metadata’ directly, but it does discuss this concept by the general term ‘electronic record’ and the authentication requirements in Section 63. In view of the evidentiary value of metadata, courts have increasingly accepted it as evidence with proper certification: In Dharambir v. CBI [(2008) 150 DLT 393], the Delhi High Court allowed computer-generated logs as evidence with appropriate certification.

4.4.2 CCTV Footage and Video Evidence

CCTV footage has specific challenges with authenticity: it can be compromised by compression, low resolution, editing of the time stamp, and conversion of the format of the footage. Where a BSA Section 79 (presumption as to electronic agreements and records) or a BSA Section 81 (presumption as to electronic messages) is in effect, the system is subject to these presumptions. In Tomaso Bruno v. State of U.P. [(2015) 7 SCC 178], the Supreme Court accepted CCTV footage as evidence of corroboration and stressed the need for a chain of custody and expert analysis of the footage.

4.4.3 Mobile Device Data and Social Media Communications

One of the most vibrant fields of digital evidence law is the preservation and admission of mobile device information: call history, WhatsApp conversations, deleted text messages retrieved via mobile device forensics, geospatial data, and so on. The Madras High Court in the case of Dharani Sugars and Chemicals Ltd. v. Union of India noted that WhatsApp messages can be admissible with the proper certification but it has to be established that the extraction of such messages is done in a manner that is proper and proper linkage with the accused has been done. While the BSA's Section 62 framework is uniform across mobile-extracted data, practical issues of end-to-end encryption can lead to being able to extract metadata but not necessarily the content of a message.

4.4.4 Cloud-Stored Evidence

Cloud computing's distributed and multi-jurisdictional design presents significant issues for digital evidence law. Amazon Web Services, Google Cloud, Microsoft Azure and other providers may store data on servers in different countries, which could raise issues around territorial jurisdiction in gathering evidence, potential issues with foreign data protection laws (such as the GDPR) and whether the Indian procedural rules would apply to foreign service providers. The BSA's Section 62 takes a pragmatic approach and allows the 'person in control' of the computer resource to certify it without having to specify any particular physical location of a server, thereby addressing the jurisdiction issue somewhat.

V. PROCEDURAL SAFEGUARDS UNDER THE BHARATIYA NAGARIK SURAKSHA SANHITA, 2023

5.1 Search, Seizure, and Preservation of Digital Evidence

The Bharatiya Nagarik Suraksha Sanhita, 2023 brings in significantly updated provisions regarding the search and seizure of electronic evidence to fill in some major gaps in the previous CrPC provisions, which were drafted before the extensive use of computers in criminal activity. Section 94 BNSS provides for the compelling production of documents and digital records, and there are new sub-provisions that specifically cover electronic devices, cloud accounts and remote servers.

The current section 185 BNSS is complemented by section 186, which introduces for the first time the notion of digital search warrants, that is court orders that permit access to electronic devices, email accounts, cloud storage and encrypted data. The procedural requirements are: particular identification of the target device, specification of the categories of data sought, the limitation of the scope of the search over the course of time and required videography of the search process. Section 105 BNSS's videography requirement also has an impact on digital evidence because it will result in a contemporaneous record of the forensic acquisition process, which will enhance chain-of-custody integrity.

5.2 Chain of Custody and Digital Forensic Standards

The chain of custody, a documented continuous chain of possession, condition and location from the time of seizure to court presentation, is critical to the integrity of digital evidence. The BNSS introduces Section 530 which requires the preparation of a 'Digital Evidence Recovery Sheet' (DERS) at the time of electronic device seizure, including identification of device (IMEI, serial number, MAC address), condition of device, storage capacity and contents, device encryption, and forensic acquisition technique used.

In addition, the BNSS requires, in Section 531, that all digital evidence handling be done with write-blocking equipment to ensure that any original data is not accidentally altered, and that a forensic image (bit-for-bit copy) be created prior to any analysis with hash values (MD5 or SHA-256) also calculated for both the original image and the forensic image to ensure that they are identical. Such a codification of good practice forensics is welcome progress, but the success or otherwise of the law will rely heavily on the equipment available and the training of country-wide police forensic units, which is a shortage in smaller states and union territories.

5.3 Trial Procedure and Electronic Evidence Presentation

Section 353(3) of the BNSS allows for electronic evidence to be presented at trial, allowing witnesses to testify via video link and documents to be displayed electronically, with proper authentication. With electronic filing of case documents and chargesheets under Section 530 BNSS, an all electronic evidentiary system in principle has been made possible by the BSA's electronic record provisions.

Perhaps most importantly, the BNSS has introduced a requirement for the mandatory forensic investigation of offences, where seven or more years imprisonment will be imposed, in Section 176(3): this includes the filming of the investigation of any crime scene by a forensic team. This is a measure which is in its main form directed at physical crime scenes, but which practitioners interpret as covering digital crime scenes (servers, devices, networks) in light of the definition of 'crime scene' as being integrated in the BNSS's Explanation to Section 176.

VI. LANDMARK JUDICIAL PRECEDENTS ON DIGITAL EVIDENCE

6.1 Anvar P.V. v. P.K. Basheer: The Foundational Ruling

The three-judge bench interpretation by the Supreme Court in Anvar P.V. v. P.K. Basheer [(2014) 10 SCC 473] has basically changed the rules of admissibility of electronic evidence in India. In State (NCT of Delhi) v. Navjot Sandhu (2005), the earlier division bench had clarified that secondary evidence provisions will be applicable in the admission of electronic evidence, which does not require the Section 65B certificate. The Court held otherwise,

finding the provisions of Sections 65A and 65B of the IEA to constitute a complete and self-contained code for electronic evidence. The certificate was not considered a fairly routine formality, but a condition of admission.

The ratio of Anvar P.V. set forth three important rules: first, the certificate is required to be used to give primary evidence; second, the Section 65B certificate (now Section 62 BSA) is not the oral evidence; and third, the original device does not have to be provided when the Section 65B certificate (now Section 62 BSA) is present. The principles are still the basis for the admission decisions as outlined in the BSA.

6.2 Arjun Panditrao Khotkar: Constitutional Bench Clarification

The Constitution Bench Judgement in the case of Arjun Panditrao Khotkar vs Kailash Kushanrao Gorantyal (2020) 7 SCC 1 came in the wake of differences of opinion between High Courts on the question of whether courts can condone the delay in issuing certificates. The five-judge bench unanimously ruled that the certificate is a condition precedent to the admissibility and cannot be ignored or dispensed with at the discretion of the court. Most importantly, the Court has also upheld the inherent jurisdiction of the trial courts under Section 311 CrPC (presently Section 357 BNSS) to summon the person responsible for issuing the certificate, where the certificate is not issued by the tendering party, a practice that would otherwise make it difficult to exclude evidence on the basis of a procedural error by the investigating agency.

The Court also explained the meaning of the 'responsible official position' of the person who signed the certificate, which does not require the person to be the highest-ranking position in the organisation operating the device, but rather a person who has a direct understanding of the operation of the system and the conditions under which the record was created. Where the 'responsible official' is an employee of a foreign corporation, this qualification has proven to be of particular value where social media evidence is concerned.

6.3 Subsequent Developments and High Court Jurisprudence

Post Arjun Panditrao, High Courts have elaborated and elaborated the Doctrine. The Bombay High Court in Sonu v. State of Maharashtra (2021) SCC Online Bom 887 has ruled that the CCTV footage downloaded onto a pen drive by the police investigators must have a certificate from the original CCTV system installer and not just from the police officer who had made the copy, which upsets the investigating officer. In V.D. Swamy v. State [(2022) SCC Online Mad 2341] the Madras High Court ruled that the individual who has taken the screenshots on WhatsApp should certify them, thereby holding that personal knowledge is a requirement for a screenshot. The subsequent decision in Shakti Vahini v. Union of India [(2018) 7 SCC 192] of the Supreme Court, particularly in obiter dicta, provides an important insight into the admissibility of location data from mobile towers and GPS devices, finding that such data - when properly certified and corroborated with physical evidence - has a high probative value and can be admissible under the Section 65B framework.

VII. PRACTICAL CHALLENGES IN DIGITAL EVIDENCE AND CYBERCRIME INVESTIGATION

7.1 Cross-Border Cybercrime and Jurisdictional Conflicts

The basic problem with cybercrime jurisdiction is that the lex loci delicti principle – that the law in force where the offence was committed – is not enough for crimes committed by servers in Country A, via servers in Country B, that came to the attention of victims in Country C and where perpetrators are physically located in Country D. The Indian Jurisdiction be extended to any offence committed by use of the computer, computer system or computer network which is situated in India, irrespective of the location of the offender as per the IT Act, 2000 (Section 75). The BNS also covers extraterritorial application in accordance with Section 4(3) of the BNS for offences of an extraterritorial nature that impact on the lives and property of citizens.

The mutual legal assistance treaty (MLAT) network that India has signed, 44 bilateral treaties till date, has been made available for evidence collection, however, the average MLAT request takes 12-18 months to be processed, which makes it ineffective for time-sensitive cybercrime investigations. The Budapest Convention on Cybercrime (not yet ratified by India but it was invited to be an observer in 2018) offers a more effective multilateral arrangement with provisions for speedy preservation of digital evidence. The continued non-accession of India is a major lacuna in its international Cyber law engagement.

7.2 Encryption Barriers and the Right to Silence

The use of end-to-end encryption – such as WhatsApp, Signal, Telegram (secret chats), and iMessage – raises basic issues for digital evidence retrieval. If the communication between the suspect and another party is encrypted and the platform operator doesn't have the decryption keys, interception orders under Section 69 IT Act are not able to provide intelligible information. Law enforcement has sought to respond by emphasizing metadata - who talked to whom, when and for how long - device forensics - getting the data from the device before it is encrypted for later analysis, and password forcing.

The forced-disclosure issue is a constitutional conundrum. Section 91 CrPC (now Section 94 BNSS) provides power to the courts to require production of documents such as encrypted data, but requires the person who is ordered to produce be allowed to refuse to provide a password or decryption key to unlock the information, which could impinge on the right to refrain from incriminating oneself under Article 20(3) of the Constitution. There is no clear consensus in the Supreme Court as to whether the giving of a password is ‘testimonial compulsion' for the purpose of Article 20(3). The Kerala High Court in the case of Vineeth V.S. v. State [(2021) 5 KHC 367] has ruled that compulsion to decrypt a personal device breaches Article 20(3) while the Bombay High Court in obiter has said that technical access (without humans) of personal device does not contravene Article 20(3). Such a doctrinal uncertainty clearly affects investigations.

7.3 Data Privacy and the DPDP Act, 2023

The BNS trilogy is complemented by the Digital Personal Data Protection Act, 2023 (DPDP Act), which establishes a robust framework for managing personal data and intersects with cybercrime investigations. The scope of Section 17 DPDP Act is limited, as the exemption from obligations is only for processing for ‘prevention, detection, investigation, or prosecution of any offence', which has been drafted deliberately to be as narrow as possible, and requires for the exemption to be fulfilled: necessity and proportionality. The Act generates a massive and significant conflict in evidence law where large scale data collections by law enforcement in predictive policing or network analysis can be considered as unlawful processing, which can jeopardize the admissibility of derivatively acquired evidence.

The right to data portability in DPDP Act, however, can help in digital evidence collection: in case of cybercrime, the victim can request its removal from the platform (such as logs of interactions with the perpetrators) and surrender it to investigators without having to go through the MLAT process for victim-held evidence. This mechanism is not being used to its full extent in the current investigations.

7.4 AI-Generated Evidence and Deepfake Authentication

With the rise of generative AI tools comes a new evidentiary challenge: verifying that a digital content (video, audio, image, text) is authentic and not created by a generative AI tool. The quality of AI-generated deepfakes has become close enough to the real thing that they are highly likely to be considered real without advanced forensics. While the BSA doesn't explicitly speak to AI-generated content, it does require that the general authentication rules governing traditional digital evidence apply to it.

Distributed ledger technology-based evidence authentication has proven to be a viable solution that ensures tamper-proof evidence creation, acquisition, and handling records. The technical viability of immutable evidence logs has been demonstrated in platforms such as Guardtime (Estonia), Epiq and the blockchain pilots run by the National Informatics Centre (NIC) in India. But there is, as yet, no

recognition of evidence authenticated by blockchain technology that it carries a presumption of integrity, and it is subject to general principles of admissibility.

7.5 Forensic Infrastructure Gaps

The capacity of forensic laboratories is essential to effective digital evidence utilisation. There are about 90 central and state level government forensic science laboratories (FSL) in India with only 20 FSLs having a dedicated unit with international standard of cyber forensics. There is a huge gap in the capacity in terms of specialists, with the Centre for Development of Advanced Computing (C-DAC) and Indian Computer Emergency Response Team (CERT-In) providing the same. NCRB data indicates that forensic examination backlogs in some states are as high as 3 years. The compulsory requirement for a forensic investigation under Section 176(3) BNSS will result in a significant increase of demand but not the expansion of capacity.

VIII. COMPARATIVE INTERNATIONAL FRAMEWORKS

8.1 European Union: The Budapest Convention and GDPR Interface

The Council of Europe's Budapest Convention on Cybercrime (2001) is the most widely signed international cybercrime convention (with 68 state parties) which India has not yet ratified. Chapter II of the Convention covers substantive offences (illegal access, data interference, system interference, computer-related fraud) and Chapter III protects the procedural tools such as expedited preservation orders (Article 16), production orders (Article 18) and real-time collection of traffic data (Article 20). The Convention has targeted the most practically relevant issues of evidence, in Articles 32 (transborder access to stored computer data with consent) and 33 (real-time collection across borders).

The EU's General Data Protection Regulation (GDPR) imposes a complicated layer of criminal investigations, demanding that criminal data processing adhere to necessity and proportionality tests even when processing such data is for legal purposes. The GDPR's 'Law Enforcement Directive' (Directive 2016/680) offers a more specific set of rules for criminal justice data processing. A balance between effective evidence gathering and strong data protection rights, as the EU has achieved with specific legislative exemptions, can be used as a blueprint for the evolving implementation of the DPDP Act in India.

8.2 United Kingdom: Computer Misuse Act and Investigatory Powers

The Computer Misuse Act 1990 (as amended) and the Investigatory Powers Act 2016 ('Snoopers' Charter') are a comprehensive measure that provides for surveillance powers with a degree of judicial oversight. The IPA's 'equipment interference' powers (which allow for the remote hacking of devices by security services) and its bulk personal datasets retention will be at opposite ends of the scale when it comes to evidence-gathering. The scope of the IT Act, 1939's Section 69 surveillance powers is wide but lacks a systematic judicial authorisation and oversight mechanism similar to what the IPA has in place through warrant and commissioner.

8.3 United States: Federal Rules and the CLOUD Act

This new law, called the Clarifying Lawful Overseas Use of Data (CLOUD) Act of 2018, answered the question that long plagued the industry of whether US law enforcement could force American businesses to produce data that is stored outside the country. It also has an executive agreement mechanism which allows for bilateral data-sharing arrangements without having to go through MLAT delays. India and US are negotiating an executive agreement under the CLOUD Act that will hasten the retrieval of digital evidence for investigators in India in numerous cybercrime cases that involve platforms based in the US. US Federal Rules of Evidence Rule 901(b)(9) 'authentication by evidence describing a process or system' has had a significant impact on courts around the world in their approach to the authentication of digital evidence systems.

IX. PROPOSED REFORM FRAMEWORK

9.1 Legislative Recommendations

This paper suggests the following legislative measures for enhancing the digital justice ecosystem in India:

- The implementation of a specific Cyber Crime Act that brings together the provisions of the BNS, IT Act, DPDP Act and BNSS by establishing a single law that includes specific offences for ransomware, deepfakes, cryptocurrency fraud, automated bot attacks and crimes involving IoT devices.
- Access to the Budapest Convention on Cybercrime for fast-track access to mutual legal assistance and cross-border preservation of evidence, with appropriate reservations to bulk surveillance provisions.
- Eliminates burden and certification requirements while maintaining standards for electronic records, with a rebuttable presumption of integrity for blockchain-authenticated electronic records.
- The statutory introduction of a 'Digital Evidence Custodian' in investigative agencies to personalise a role and establish standards of professionalism for all those handling digital evidence within an investigation.
- Legislative recognition of AI detection forensics as expert evidence and the setting of standards for court-appointed AI forensic experts and the admissibility of AI content authentication reports.
- Amendment to the DPDP Act to define the scope of the law enforcement exemption, to establish a structured approach to data requests made by investigators, to guarantee efficient requests while safeguarding privacy.

9.2 Institutional and Technological Recommendations

- Building a National Digital Evidence Laboratory (NDEL) under the Ministry of Home Affairs with regional centres in each state, having state-of-the-art forensic hardware and software, ISO 17025 accreditation and inter-operability with international forensic databases.
- National Digital Chain of Custody System (NDCCS), a government-operated blockchain platform to document and validate all stages of the digital evidence process, from its seizure to its presentation in court, establishing an unalterable record of evidence.
- Establishment of a Cyber Court Infrastructure Programme under e-Courts Mission Mode Project, creation of cyber courts in every district with facilities for presentation of evidence in court in a secure manner, a facility for live forensic expert testimony and a facility to manage exhibits in an encrypted manner.
- An AI-Assisted Investigation Platform (AAIP) developed and supervised by CERT-In that incorporates AI-based tools for malware attribution, network traffic analysis, social media pattern recognition, and deepfake detection, with access restrictions and judicial authorisation for creating investigative outputs with AI.
- The establishment of training programs for law enforcement digital forensics based on the EC-Council's Certified Computer Examiner (CCE) or equivalent national standard, and periodic re-certification to ensure that these officers stay abreast of evolution in technology.
- Cooperation: bilateral CLOUD Act executive agreements with the United States, the United Kingdom, the European Union and Singapore, increased engagement with Interpol and FATF regarding cryptocurrency crime, and modernization of MLAT to ensure a response to urgent evidence preservation requests in under 30 days.

9.3 Judicial Capacity Building

- Incorporation of compulsory training in digital evidence for all judicial officers at the National Judicial Academy with hands-on courses on interpretation of forensic reports, identifying a deepfake, tracking cryptocurrency and expert witness cross-examination.
- The Independent Digital Forensic Examiners (IDFEs) will be appointed by the court in complex cyber cases in cases where both prosecution and defence offer conflicting evidence, similar to the commissioners appointed under Section 484 BNSS, with a view to supplying technical expertise in a neutral manner.
- The Supreme Court E-Committee in collaboration with CERT-In, C-DAC and the Bar Council of India, prepared a Judicial Benchbook on Digital Evidence which is a comprehensive reference book for trial courts and is updated on an annual basis to take care of technological advancements.

X. CONCLUSION

The Bharatiya Nyaya Sanhita, Bharatiya Nagarik Suraksha Sanhita and Bharatiya Sakshya Adhiniyam, 2023 are the most ambitious reforms in criminal law since independence. These laws make meaningful strides in the area of cyber crime and digital evidence: the BSA's new electronic records rules, the BNSS's requirement for forensic investigations, and the new technology neutral section of the BNS, which extends criminal liability.

But the chasm between the law and its implementation is still too large. India's forensic science labs, the judiciary, with regard to the international cooperation mechanisms and consistency of procedure across the country's 29 states and the eight UTs are lacking in the ability to create a credible electronic justice system. Those are good concepts, and perhaps the law will be strong enough to enforce them as long as the police officer knows how to preserve the evidence without contamination, the forensic examiner is able to authenticate the evidence and the judge is ready to evaluate the evidence.

As India strives to become a $1 trillion economy, the nation's cybercrime surface will be growing in tandem. While the BNS trilogy is a foundation, the building of a digital justice requires constant attention of the legislature, significant institutional investments, and cultural change in both the practice of law and law enforcement. The steps outlined in this paper — a specially drafted Cyber Crime Act, national digital evidence infrastructure, CLOUD Act engagement and judicial capacity development — are the next steps in this unfinished narrative.

In the end, digital justice is not just a technical issue, it's a constitutional one. Article 21's right to life and personal liberty extends to citizens' digital lives, while the equality clause in Article 14 requires uniform treatment across the sprawling geography of India in evidence gathering by the police. The Bharatiya law trinity of 2023 has charted the course, and the march towards digital justice has just begun.

REFERENCES

[1] National Crime Records Bureau, Crime in India 2023: Cyber Crime Report (Ministry of Home Affairs, 2024).

[2] Information Technology Act, 2000 (Act 21 of 2000), as amended in 2008.

[3] Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).

[4] Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).

[5] Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

[6] Indian Penal Code, 1860 (Act 45 of 1860).

[7] Indian Evidence Act, 1872 (Act 1 of 1872).

[8] Code of Criminal Procedure, 1973 (Act 2 of 1974).

[9] Indian Penal Code, 1860 (Act 45 of 1860).

[10] Indian Penal Code, 1860 (Act 45 of 1860).

[11] Information Technology Act, 2000 (Act 21 of 2000), as amended in 2008.

[12] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (Supreme Court of India).

[13] Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).

[14] Tukaram S. Dighole v. Manikrao Shivaji Kokate, (2010) 4 SCC 329 (Supreme Court of India).

[15] Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).

[16] Information Technology Act, 2000 (Act 21 of 2000), as amended in 2008.

[17] Avnish Bajaj v. State (NCT of Delhi), (2008) 150 DLT 769 (Delhi High Court).

[18] Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).

[19] National Crime Records Bureau, Crime in India 2023: Cyber Crime Report (Ministry of Home Affairs, 2024).

[20] Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).

[21] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (Supreme Court of India).

[22] Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).

[23] Information Technology Act, 2000 (Act 21 of 2000), as amended in 2008.

[24] Indian Evidence Act, 1872 (Act 1 of 1872).

[25] Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

[26] Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

[27] Indian Evidence Act, 1872 (Act 1 of 1872).

[28] Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

[29] Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

[30] Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

[31] Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

[32] Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

[33] Information Technology Act, 2000 (Act 21 of 2000), as amended in 2008.

[34] Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

[35] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (Constitution Bench).

[36] Tomaso Bruno v. State of U.P., (2015) 7 SCC 178 (Supreme Court of India).

[37] Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

[38] Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

[39] Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

[40] Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).

[41] Code of Criminal Procedure, 1973 (Act 2 of 1974).

[42] Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).

[43] Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).

[44] Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).

[45] Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).

[46] National Crime Records Bureau, Crime in India 2023: Cyber Crime Report (Ministry of Home Affairs, 2024).

[47] Ministry of Home Affairs, Report of the Expert Committee on Cyber Crime Investigation Standards (2022).

[48] Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).

[49] Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).

[50] Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

[51] Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).

[52] Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).

[53] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (Supreme Court of India).

[54] State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600 (Supreme Court of India).

[55] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473 (Supreme Court of India).

[56] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (Constitution Bench).

[57] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (Constitution Bench).

[58] Sonu v. State of Maharashtra, (2021) SCC Online Bom 887 (Bombay High Court).

[59] V.D. Swamy v. State, (2022) SCC Online Mad 2341 (Madras High Court).

[60] Shakti Vahini v. Union of India, (2018) 7 SCC 192 (Supreme Court of India).

[61] Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).

[62] Information Technology Act, 2000 (Act 21 of 2000), as amended in 2008.

[63] Council of Europe, Convention on Cybercrime (Budapest Convention), ETS No. 185 (2001).

[64] Information Technology Act, 2000 (Act 21 of 2000), as amended in 2008.

[65] Vineeth V.S. v. State, (2021) 5 KHC 367 (Kerala High Court).

[66] Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

[67] Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

[68] Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

[69] Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

[70] Ministry of Home Affairs, Report of the Expert Committee on Cyber Crime Investigation Standards (2022).

[71] National Crime Records Bureau, Crime in India 2023: Cyber Crime Report (Ministry of Home Affairs, 2024).

[72] Ministry of Home Affairs, Report of the Expert Committee on Cyber Crime Investigation Standards (2022).

[73] Council of Europe, Convention on Cybercrime (Budapest Convention), ETS No. 185 (2001).

[74] Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

[75] UNODC, Comprehensive Study on Cybercrime (United Nations Office on Drugs and Crime, 2013, updated 2022).

[76] Information Technology Act, 2000 (Act 21 of 2000), as amended in 2008.

[77] UNODC, Comprehensive Study on Cybercrime (United Nations Office on Drugs and Crime, 2013, updated 2022).

[78] Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).

[79] Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).

[80] Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

[81] Information Technology Act, 2000 (Act 21 of 2000), as amended in 2008.

[82] Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

[83] Council of Europe, Convention on Cybercrime (Budapest Convention), ETS No. 185 (2001).

[84] Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

[85] Ministry of Home Affairs, Report of the Expert Committee on Cyber Crime Investigation Standards (2022).

[86] Ministry of Home Affairs, Report of the Expert Committee on Cyber Crime Investigation Standards (2022).

[87] Digital Personal Data Protection Act, 2023 (Act 22 of 2023).

[88] Ministry of Home Affairs, Report of the Expert Committee on Cyber Crime Investigation Standards (2022).

[89] Ministry of Home Affairs, Report of the Expert Committee on Cyber Crime Investigation Standards (2022).

[90] Law Commission of India, 248th Report: Obsolescence of the Evidence Act and Need for Reform (2014).

[91] CERT-In, Annual Report 2023-24 (Ministry of Electronics and Information Technology, 2024).

[92] Ministry of Home Affairs, Report of the Expert Committee on Cyber Crime Investigation Standards (2022).

[93] Council of Europe, Convention on Cybercrime (Budapest Convention), ETS No. 185 (2001).

[94] UNODC, Comprehensive Study on Cybercrime (United Nations Office on Drugs and Crime, 2013, updated 2022).

[95] Law Commission of India, 248th Report: Obsolescence of the Evidence Act and Need for Reform (2014).

[96] Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).

[97] Law Commission of India, 248th Report: Obsolescence of the Evidence Act and Need for Reform (2014).

[98] CERT-In, Annual Report 2023-24 (Ministry of Electronics and Information Technology, 2024).

[99] Law Commission of India, 248th Report: Obsolescence of the Evidence Act and Need for Reform (2014).

[100] Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).

[101] Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).

[102] Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

[103] National Crime Records Bureau, Crime in India 2023: Cyber Crime Report (Ministry of Home Affairs, 2024).

[104] Ministry of Home Affairs, Report of the Expert Committee on Cyber Crime Investigation Standards (2022).

[105] Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).

[106] Bharatiya Nagarik Suraksha Sanhita, 2023 (Act 46 of 2023).

[107] Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023).

[108] Parliamentary Standing Committee on Home Affairs, 227th Report on the Bharatiya Nyaya Sanhita Bill, 2023 (Rajya Sabha Secretariat, 2023).