THE ADMISSIBILITY AND EVIDENTIARY CHALLENGES OF DIGITAL EVIDENCE IN INDIAN CRIMINAL TRIALS

Sahina FirozAlam Nai*

ABSTRACT

The rapid digitisation of society has transformed the landscape of criminal wrongdoings, making digital evidence an essential element of modern-day criminal trials. This paper critically examines and analysis the complex challenges surrounding the admissibility, authentication, and integrity of digital evidence within the Indian criminal justice system, particularly in light of the recently enacted Bhartiya Sakshya Adhiniyam,2023(herein after BSA) through a doctrinal study of the BSA's provisions relevant landmark precedents(developed under the erstwhile Indian Evidence Act(herein after IEA), 1872, and their applicability under the new laws) and the Information Technology Act, 2000. It delves into the evolving judicial interpretations, including the pivotal role of Section 65B of the IEA, which deals with certification, and differentiates digital evidence's characteristics and significant requirements from traditional physical evidence. This paper argues that although the legal framework has amended itself and has adapted, ambiguities, a lack of uniform forensic protocols, and a dynamic approach to justice, it has created significant hurdles for effective justice delivery. The paper highlights how the unique attributes of digital information, such as its unpredictability, intangibility, and susceptibility to alteration or even bias, present challenges that are distinct from those of the traditional physical evidence. Ultimately, it proposes comprehensive legislative and procedural reforms, along with enhanced judicial and law enforcement training among the legal practitioners, to make legal principles compatible with technological realities, thereby ensuring fair, efficient, and technologically capable adjudication of criminal matters in India.

Keywords: Digital Evidence, Admissibility, Cyber Crime, Procedural Reforms.

*BA LLB, SECOND YEAR, RIZVI LAW COLLEGE.

INTRODUCTION

The creation of internet-enabled devices with digital connectivity has transformed society into an unpredictable era of virtual interactions and the exchange of information. This digitalisation has not only revolutionised society but has also been accompanied by increased crime. There is a reported shift of traditional crimes to much more complex scenes, including the digital environment. It has necessitated a reevaluation of the legal framework of modern India, especially the one governing evidence. Due to the significant contribution of digitalisation in the advancement of the methods of crimes, it not only increases the judiciary's reliance on digital evidence but also underscores the need for a robust framework surrounding the reliability and admissibility of such evidence. This is a crucial agenda for the judicial system of India, given that the societal impact of digital presence in society, making digital evidence an indispensable component of criminal trials, as the *IEA (1872*) had defined.

Evidence: As Oral and Documentary: However, due to the onset of digital revolution with far-reaching consequences for individuals, there has to be fundamental shift to accommodate the digital records as evidences too, although the clear necessity digital documents to be admissible as evidences, they pose several challenges including votality, intangibility and ease to alteration of the data required to be brought on record making it different from the physical evidences. The IEA, 1872, is historically inadequate to address such evidence, which, being digital evidence, has undergone significant amendments with the introduction of the new law of Bhartiya Sakshya Adhiniyam (hereinafter BSA,2023). The BSA came into force on 1st of July 2024, replacing the old IEA,1872, depicting a notable legislative advancement through modernising laws governing evidence for the digital age, whilst aiming to ensure speedy justice, enhanced accountability, and transparency in investigations, and foster a more victim-centric Criminal Justice System. The BSA notably recognises and provides a framework for the admissibility and reliability of digital records as evidence. Despite the advancements brought by the BSA, 2023, the process of authenticating, ensuring the integrity and genuineness, and admitting digital records as evidence continues to present complex challenges. In trials, these challenges originate from the changing fundamentals of digital data, evolving digital landscapes, and the need for consistent application of the new law. This paper aims to address: the BSA’s provisions and implications the key judicial precedents that has shaped the admissibility standards for the digital records as evidences, , and other challenges, practical and procedural complexities in acceptance and handling of the digital evidences, and

to various stakeholders of the legal practice, and opportunities brought up by this revolutionized digital age through a thorough comparison, which can highly contribute as evidence in criminal trials, whilst providing insights and recommendations.

THESIS STATEMENT

While the Bharatiya Sakshya Adhiniyam, has been complemented by procedural advancements in the BNSS, this step represents a leap which is significant legislative leap by classifying digital evidence as primary evidence and revolutionizing the related provisions, although the above it is still accompanied by persistent ambiguities within its provisos with continued lack of standardization in the forensic protocols, lack and consistent need for judicial precedents to interpret the new concepts, with the inherent technical distinctions from physical evidence it necessitates an urgent procedural enhancements accompanied by specialized training, and other necessary initiatives to ensure a fair and effective delivery of justices in this digital age.

METHODOLOGY

This paper employs a mixed methods approach, with a primary focus on doctrinal analysis, supplemented by a primary data collection method (survey).

Doctrinal Analysis-

Doctrinal analysis shall provide an in-depth examination of statutes and the legal framework governing digital evidence in India. At the same time, the survey will also provide an additional insight into the practicalities of this matter and various perceptions of the legal practitioners, and will involve a critical examination of primary sources, including

Statutes: Bharatiya Sakshya Adhiniyam, 2023-24(hereinafter BSA), Bhartiya Nagarik Suraksha Sanhita, 2023-24 (hereinafter BNSS), Bharatiya Nyaya Sanhita, 2023-2(hereinafter BNS)

Case Law: Landmark judgments related to digital evidence in Indian courts

Constitutional Provisions: Relevant provisions of the Indian Constitution. The analysis will also draw upon secondary sources, including articles, books, and reports.

Primary Data Collection through Survey (Supplementary): A survey has been conducted to gather primary data from legal professionals. The survey aimed to gather data on their experiences and perceptions regarding digital evidence in Indian criminal trials.

Justification for Methodology: The mixed methods of doctrinal analysis and primary data collection through a survey are justified because they allow for a comprehensive understanding of the legal framework surrounding the admissibility of digital evidence in India, as well as the practical experiences and perceptions of legal professionals. The doctrinal analysis provides a thorough examination of the legal principles and rules, while the survey offers additional insights into the practical challenges and opportunities presented by digital evidence. Furthermore, by combining these methods, this research aims to provide insights into the implications of electronic evidence for the fair and effective administration of justice in this revolutionised digital age.

STATUTORY FRAMEWORK FOR DIGITAL EVIDENCE IN INDIA

With the onset of a revolutionized digital age, there has been a new legal framework introduced in the India's criminal justice system marking a significant shift, and reflecting upon the evolving nature of laws, specifically the criminal laws in India, inter alia, the Bharatiya Nyaya Sanhita (BNS), 2024 which replaces the Indian penal code (IPC), 1860, the Bharatiya Nagarik Suraksha Sanhita(BNSS) replacing the code for criminal procedure, CrPC, and the Bharatiya Sakshya adhiniyam (BSA) which replaces the Indian evidence act, (IEA), 1872, these recent legislative changes provides for a revised framework of the justice system and aims to modernize its provisions to deal with the complexities of the technology.

THE INDIAN EVIDENCE ACT, 1872: HISTORICAL AND CONTEMPORARY ANALYSIS

The Indian Evidence Act, enacted in the year 1872, acts as the core legislation that provides for the regulations revolving around the admissibility and evaluation of evidence in the Indian justice system. Whilst being predated by the digital age, this framework has provisions which with certain limitations and challenges, have tried to accommodate digital evidence, this act has been stretched to fit digital records, often leading to legal ambiguities and inconsistencies, this arose the need to have a more comprehensive and technologically-neutral frameworks, paving a way for the introduction of the BSA.

Section 3 of the Indian Evidence Act, 1872: Section 3 defined "evidence" as all statements that the court permits or requires to be made before it.[1]. This definition includes both oral and documentary evidence, leaving room for different interpretations regarding the admissibility and evaluation of the digital records as evidence.

Section 65B of the Indian Evidence Act: Section 65B of the Indian Evidence Act, 1872 mandates a certificate signed by a person in a reasonable position related to the electronic device or its operation for the admissibility of electronic records as evidence in court.[2] It is evident that in contemporary times, the Indian justice system has faced significant challenges in accommodation od digital evidence, the provisions of this act have been stretched to fit in the digital records as evidence, often leading into legal ambiguities and inconsistencies, arising a need for technology-neutral legal framework, paving the way for introduction of the new laws.

BHARATIYA SAKSHYA ADHINIYAM (BSA) 2024

Defining Digital Evidence Under The BSA Is Crucial for Understanding How Digital Evidence Is Legally Defined and Treated Under the New Laws.

Definitions: (Incorporated from the Bare Act)

Section 2(1) (D) of BSA Definition of Document: Section (d) "document" means any matter expressed or described or otherwise recorded upon any substance using letters, figures or marks or any other means or by more than one of those means, intended to be used, or which may be used, to record that matter and includes electronic and digital records.*Illustrations.* (i) A writing is a document. (ii) Words printed, lithographed, or photographed are documents. (iii) A map or plan is a document. (iv) An inscription on a metal plate or stone is a document. (v) A caricature is a document. (vi) An electronic record on emails, server logs, documents on computers, laptops, or smartphones, messages, websites, locational evidence, and voice mail messages stored on digital devices is are document.[3]

Section 2(1) (e) of the Bharatiya Sakshya Adhiniyam (BSA) 2024: Section 2(e) states "evidence" as means and includes-- (i) all statements including statements given electronically

[1] Indian Evidence Act, 1872, S 3("Evidence")
[2] Indian Evidence Act, 1872, S 65(B)
[3] Bharatiya Sakshya Adhiniyam, 2023, Section 2(1)(D)

which the Court permits or requires to be made before it by witnesses concerning matters of fact under inquiry and such statements are called oral evidence; (ii) all documents including electronic or digital records produced for the inspection of the Court and such documents are called documentary evidence.[4]

Analysis and comparison of the definitions (Comparison with IEA): The BSA widens its approach to the digital age, expanding itself through its definitions, which would include pretty much anything electronic, making vast digital information can now be valid evidence, making the legal processes much quicker, smoother, and easier. This is a big initiative by the legislature to advance from the IEA, where it often felt like the electronic records were squeezed in, sometimes even needing extra hoops to jump through certifications.

PRIMARY AND SECONDARY EVIDENCE: (NEW CLASSIFICATION OF EVIDENCE UNDER BSA)

The BSA marks a significant shift by classifying electronic records as primary evidence under specific conditions, unlike the provisos of IEA, which generally classified electronic records as secondary evidence.

Section 57 of BSA Primary evidence-

Primary evidence means the document itself produced for the inspection of the Court.

Explanation 1: Where a document is executed in several parts, each part is primary evidence of the document.

Explanation 2: Where a document is executed in counterpart, each counterpart being executed by one or some of the parties only, each counterpart is primary evidence as against the parties executing it

Explanation 3: Where several documents are all made by one uniform process, as in the case of printing, lithography, or photography, each is primary evidence of the contents of the rest; but, where they are all copies of a common original, they are not primary evidence of the contents of the original.

[4] Bharatiya Sakshya Adhiniyam, 2023, Section Section 2(1)(E)

Explanation 4: Where an electronic or digital record is created or stored, and such storage occurs simultaneously or sequentially in multiple files, each such file is primary evidence.

Explanation 5: Where an electronic or digital record is produced from proper custody, such electronic and digital record is primary evidence unless it is disputed.

Explanation 6: Where a video recording is simultaneously stored in electronic form and transmitted or broadcast, or transferred to another, each of the stored recordings is primary evidence.

Explanation 7: Where an electronic or digital record is stored in multiple storage spaces in a computer resource, each such automated storage, including temporary files, is primary evidence.**Illustration** A person is shown to have been in possession of several placards, all printed at one time from one original. Any one of the placards is primary evidence of the contents of any other, but no one of them is primary evidence of the contents of the original.[5]

Section 58 of BSA: Secondary Evidence: Secondary evidence includes-- (i) certified copies given under the provisions hereinafter contained; (ii) copies made from the original by mechanical processes which in themselves ensure the accuracy of the copy, and copies compared with such copies; (iii) copies made from or compared with the original (iv) counterparts of documents as against the parties who did not execute them; (v) oral accounts of the contents of a document given by some person who has himself seen it; (vi) oral admissions; (vii) written admissions; (viii) evidence of a person who has examined a document, the original of which consists of numerous accounts or other documents which cannot conveniently be examined in Court, and who is skilled in the examination of such documents. *Illustration* (a) A photograph of an original is secondary evidence of its contents, though the two have not been compared, if it is proved that the thing photographed was the original. (b) A copy compared with a copy of a letter made by a copying machine is secondary evidence of the contents of the letter, if it is shown that the copy made by the copying machine was made from the original. (c) A copy transcribed from a copy, but afterwards compared with the original, is secondary evidence; but the copy not so compared is not secondary evidence of the original, although the copy from which it was transcribed was compared with the original. (d)

[5] Bharatiya Sakshya Adhiniyam, 2023, Section 57

Neither an oral account of a copy compared with the original, nor an oral account of a photograph or machine-copy of the original, is secondary evidence of the original.[6]

Analysis: These provisions radically classify the evidence as primary and secondary evidence. Classification of electronic records as primary evidence potentially bypasses the need for a certificate unless its authenticity is disputed, whilst section 58 dealing with secondary evidence overall constitutes digital copies made through mechanical processes, which ensures accuracy.

Section 63(4) of the Bharatiya Sakshya Adhiniyam (BSA) 2024: Admissibility of the electronic records and certificate.

Section 63(4) (Equivalent To The Old Section 65B Of The IEA) Admissibility Of Electronic Records

(1) Notwithstanding anything contained in this Adhiniyam, any information contained in an electronic record which is printed on paper, stored, recorded or copied in optical or magnetic media or semiconductor memory which is produced by a computer or any communication device or otherwise stored, recorded or copied in any electronic form (hereinafter referred to as the computer output) shall be deemed to be also a document, if the conditions mentioned in this section are satisfied about the information and computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence or any contents of the original or of any fact stated therein of which direct evidence would be admissible.

(2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely:--- (a) the computer output containing the information was produced by the computer or communication device during the period over which the computer or Communication device was used regularly to create, store or process information for the purposes of any activity regularly carried on over that period by the person having lawful control over the use of the computer or communication device; (b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer or Communication device in the ordinary course of the said activities; (c) throughout the material part of the said period, the computer or communication device was operating properly or, if not, then in respect

[6] Bharatiya Sakshya Adhiniyam, 2023, Section 58

of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and (d) the information contained in the electronic record reproduces or is derived from such information fed into the computer or Communication device in the ordinary course of the said activities.

(3) Where over any period, the function of creating, storing or processing information for any activity regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed using one or more computers or communication device, whether-- (a) in standalone mode; or (b) on a computer system; or (c) on a computer network; or (d) on a computer resource enabling information creation or providing information processing and storage; or (e) through an intermediary, all the computers or communication devices used for that purpose during that period shall be treated for this section as constituting a single computer or communication device; and references in this section to a computer or communication device shall be construed accordingly.

(4) In any proceeding where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things shall be submitted along with the electronic record at each instance where it is being submitted for admission, namely:- (a) identifying the electronic record containing the statement and describing the manner in which it was produced; (b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer or a communication device referred to in clauses (a) to (e) of sub-section (3); (c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person in charge of the computer or communication device or the management of the relevant activities (whichever is appropriate) and an expert shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it in the certificate specified in the Schedule.

(5) For this section, (a) information shall be taken to be supplied to a computer or communication device if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) using any appropriate equipment; (b) a computer output shall be taken to have been produced by a computer or communication device whether it was produced by it directly or (with or without human intervention) using

any appropriate equipment or by other electronic means as referred to in clauses (a) to (e) of sub-section (3).[7]

Analysis: Section 63(4)(equivalent to the old section 65B of the IEA) mandates the submission of a certificate, **signed by a person in charge of the computer or communication device and an expert, along with the electronic record.**

Interplay of Section 57 and Section 63: The potential ambiguity created by the BSA's proviso to classify electronic records as primary evidence under Section 57(only when produced following all the conditions such as "PROPER CUSTODY and is UNDISPUTED"), along with the mandatory requirement of section 63 certification, which appears to be a complete comprehensive code for the admissibility of the "computer output"(often secondary electronic evidence), i.e. section 57's positioning of certain electronic records as primary evidence depicts that they might not always require to need a section 63 certificate unless the authenticity of such electronic record is not disputed. This interplay shall likely need further judicial interpretation to clarify when a certificate is mandatory, and when the primary evidence, as classified under section 57, suffices.

OTHER RELEVANT PROVISIONS IN BSA, 2024, BNSS,2024, AND IT ACT, 2000

Section 46 of BSA, 2023-24: *Section 46 of BSA,2023-24, is equivalent to the older section 45 of IEA* states, "**In civil cases, character to prove conduct imputed, irrelevant.** In civil cases, the fact that the character of any person concerned is such as to render probable or improbable any conduct imputed to him is irrelevant, except in so far as such character appears from facts otherwise relevant.

The Bharatiya Nagarik Suraksha Sanhita,2023 (BNSS): the new replacement for the CrPC, brings along significant changes in the collection, seizure, investigation, and other procedural elements

[7] Bharatiya Sakshya Adhiniyam, 2023, S 63(4)

Electronic Fir and Summons: The BNSS now provides for the registration of First Information Reports (FIRs) as per section 173(1)(ii)[8] and issuance of summons electronically as per section 64(2)[9] of BNSS,(3(a).[10]

Mandatory Forensic Investigation: The BNSS mandates under SECTION 176(3)(b)[11], for the forensic investigation for offences punishable with 7 years of imprisonment or more, i.e. the forensic experts are required to visit the crime scene to collect forensic evidence and additionally must record the entire process of forensic investigation using mobile phones or other electronic devices capable of recording.[12]

Videography Of Search And Seizure Operations (Section 105 And Proviso To Section 185(2) Bnss): [13]The BNSS now mandates the I.O. to audio-video record the whole search and seizure process, using electronic devices, preferably using mobile phones. This is to ensure enhanced accountability through transparency, to detect if any fabrication of evidence is done, and to ensure the presence of witnesses.[14] Electronic evidence collection and production of the electronic devices, which likely contain digital evidence for investigation, inquiry, or trial.

Information Technology Act, 2000 (It Act)

Sections 4 and 5 of the IT ACT, 2000 provide for Legal Recognition of electronic records and signatures, ensuring their validity and enforceability.[15]

Section 79(A) Of The IT Act: (Examiner Of Electronic Evidence)-

79A. Central Government to notify Examiner of Electronic Evidence: The Central Government may, to provide expert opinion on electronic form evidence before any court or other authority specified, by notification in the Official Gazette, any Department, body or

[8] Bharatiya Nagarik Suraksha Sanhita,2023, S 173(1)(Ii)
[9] Bharatiya Nagarik Suraksha Sanhita,2023, S 64 (2)
[10] Standard Operating Procedure(Sop) For Audio-Visual Recording Of Scene Of Crime, Bureau Of Police Research & Development <Https://Bprd.Nic.In/Uploads/Pdf/Sop%20of%20audio%20video%20recording%20of%20scene%20of%20crime.Pdf Accessed 23 July 2025>
[11] Bharatiya Nagarik Suraksha Sanhita,2023, S 176(3)(B
[12] Standard Operating Procedure(Sop) For Audio-Visual Recording Of Scene Of Crime,Bureau Of Police Research & Development <Bprd.Nic.In>
[13] Bharatiya Nagarik Suraksha Sanhita,2023, S
[14] A Handbook For Police Officers On Bnss,2023,(Highlighting Keyprovison Changes)Maharaja Ranjit Singh, Punjab Police Academy, Philaur
[15] Information Technology Act, 2000, S 4 & S 5

agency of the Central Government or a State Government as an Examiner of Electronic Evidence.

Explanation: For this section, "electronic form evidence" means any information of probative value that is either stored or transmitted in electronic form and includes computer evidence, digital audio, digital video, cell phones, and digital fax machines.][16]

JUDICIAL PRECEDENTS AND INTERPRETATIONS

Judicial interpretations play a crucial role in shaping the justice system, specifically shaping the admissibility of electronic evidence under the evidence-governing acts of the Indian courts.

The Legacy of the Indian Evidence Act, 1872: Pre-BSA Jurisprudence: The Indian Evidence Act, 1872, has governed for over a century the admissibility of evidence in India's justice system, paving the way for several landmark precedents under its regime, and shaping the legal landscape for digital evidence. A thorough understanding of these precedents is crucial for interpreting their applicability under the regime of the new laws, specifically BSA,2024

State of Maharashtra V. Dr. Praful B. Desai (2003): In State of Maharashtra v. Dr. Praful B. In Desai, the Bombay High Court dealt with the admissibility of computer printouts as evidence. The Hon'ble High Court of Bombay held that computer printouts are admissible under section 65B of the IEA,1872, provided that all the procedural conditions are satisfied.[17]. The Hon'ble High Court of Bombay also expressed the importance of establishing the authenticity and integrity of the computer-generated documents through proper procedural certification and verification.

State (NCT of Delhi) v. Navjot Sandhu (2005): In State (NCT of Delhi) v. Navjot Sandhu, a case related to the Parliament attack, the Hon'ble Supreme Court addressed the concern for the admissibility of electronic evidence and emphasised the significance of ensuring its authenticity and reliability. The Hon'ble Court held that electronic evidence must be proved by the provisions of the IEA,1872, i.e., under section 65B, which was directory (not mandatory), along with following the IT ACT,2000. The Hon'ble Court, by taking a liberal approach, ensured that crucial evidence was not ignored/excluded on mere technicalities. The Hon'ble

[16] Information Technology Act, 2000, S 79(A)
[17] State Of Maharashtra V. Dr Praful B Desai (2004) 4 Scc 601

Court introduced a doctrine of "SUBSTANTIAL COMPLIANCE", and through this judgment, the Hon'ble SC has reaffirmed the principles of evidentiary law while recognising the unique challenges posed by electronic evidence in legal proceedings, along with highlighting the need for a flexible approach in dealing with the emerging developments.[18]

The Paradigm shift: Anvar P.V. v. P.K. Basheer (2014),10 SCC 473: In this landmark case of Anvar P.V. v. P.K. Basheer, the Hon'ble SC clarified the requirements for the admissibility of electronic evidence under Section 65B of the Indian Evidence Act, 1872, as introduced by the Information Technology Act, 2000, and pronounced it was "a COMPLETE CODE" in itself for the admissibility of electronic records. The Hon'ble Court expressed the necessity of complying with the procedural requirements as outlined in Section 65B, including the mandatory certification of electronic evidence. It also held that electronic evidence must be accompanied by a certification that affirms its authenticity and integrity. The certification must be issued by a person who has relevant 2wqtechnical expertise. The Hon'ble SC, through this decision, has laid down a landmark precedent for the admissibility of electronic records as evidence in the Indian court and highlighted the significance of procedural compliance for ensuring their reliability.[19]

Navigating the Mandate-Shafhi Mohammad v. State of Himachal Pradesh (2018): In Shafhi Mohammad v. State of Himachal Pradesh, the Hon'ble SC laid down the clarified requirement of mandatory certification under section 65B, for admissibility of the electronic evidence; furthermore, the Hon'ble court also emphasised the importance of strict compliance with the procedural requirements. Furthermore, the Hon'ble SC reaffirmed the importance of certification under section 65 B. The Hon'ble SC attempted to carve out exceptions to the mandatory certification requirement, precisely when the said data is with third parties or with the accused. The Hon'ble SC considered and upheld the "INTERESTS OF JUSTICE" argument, which suggested the exceptions for the mandatory certificate requirement of the Certificate under sec. 65B of IEA,1872, to prevent miscarriage of justice, creating a temporary deviation from Anvar P.V. ruling.[20]

Arjun Panditrao Khotkar V. Kailash Kushanrao Geranyl (2020): This case revolved around a dispute over the admissibility of the evidences in electronic form that is in the form

[18] State (Nct Of Delhi) V. Navjot Sandhu(2005) 11 Scc 600
[19] Anvar P.V. V. P.K. Basheer(2014),10 Scc 473
[20] Shafhi Mohammad V State Of Himachal Pradesh (2018) 2 Scc 801 (Sc)

of emails, with the primary issue of whether the mandatory requirement of a certificate under Section 65B(4) of the IEA, 1872, could be dispensed with regards to the argument of 'INTERESTS OF JUSTICE", as in Shafhi Mohammad ruling. This case is marked as the crucial pre-BSA judgment, in which the Hon'ble SC in its judgment provided significant clarity by reaffirming the mandatory requirement of a Section 65B(4) certificate for the admissibility of the electronic evidence, emphasising its importance for authenticity and reliability. Additionally the hon'ble SC provided guidelines for obtaining certificates could be obtained by the court orders(Section 185-190 of BNSS, regarding production of documents, which corresponds to old CrPC sections 91-92), particularly when the data is with third party/parties or the accused, the hon'ble SC further provided with clarifications for the roles of 'PRODUCER' and 'PERSON IN CHARGE OF THE COMPUTER' about the certificate, thereby through this judgment the Hon'ble reinforced the principles established in the Anvar P.V. ruling, and also underscored the Hon'ble SC's commitment to ensure the reliability and authenticity of the electronic evidence.[21] These precedents have carved out the landscape of laws related to digital evidence in India, and they continue to influence the judicial reasoning under the BSA.

Interpreting Past Precedents under the BSA: BSA implies introducing new provisions and classifications for digital evidence, which has through its introduction, has brought in significant changes in the interpretation of digital evidence in the Indian justice system. Its provisions, particularly Sections 57 and 63, are poised to fundamentally alter the applications of the existing jurisprudence, most notably the pronouncements given by the Hon'ble SC in the ruling of Anvar P.V. and the ruling of Arjun Panditrao Khotkar. Section 57 of the BSA widens the concept of 'primary evidence' to include various electronic records, such as those from 'proper custody' unless disputed. Section 57 of the BSA explanation 5 states that "where an electronic or digital record is produced from proper custody, such electronic and digital evidence is primary evidence unless it is disputed". This means that if an electronic and digital record qualifies the above given criteria as primary evidence without its authenticity and custody being challenged, the mandatory certificate previously required under section 65B(4)of the IEA, 1872(now section 63(4) of BSA) may no longer be necessary, this shifts the charge, where the disputed nature of evidence, rather than its electronic format alone, triggers the need for a certificate. However, the section 63(4) certificate remains crucial for secondary electronic

[21] Arjun Panditrao Khotkar V Kailash Kushanrao Gorantyal (2020) 7 Scc 1

records, or when the conditions of primary status of evidence as contested in section 57, explanation 5 of the BSA, are not met.

This change to the new legal framework is likely to cause initial confusion in trial courts as they harmonise the provisions of the BSA with the established jurisprudence. Key challenges include interpreting "proper custody" in this digital age, defining what constitutes a valid "dispute" under section 57, explanation 5, and adaptation of the provided procedural norms. There is a high need for new judicial pronouncements, i.e., the Hon'ble courts will eventually, through their judgments will need to provide for authoritative interpretations of the BSA's digital evidence provisions, especially the ones encircling the interplay of Sections 57 and 63.

DIGITAL EVIDENCE VS. PHYSICAL EVIDENCE: A COMPARATIVE ANALYSIS OF EVIDENTIARY HANDLING

Fundamental distinction between Digital evidence and Physical evidence lies in their Inherent Nature, i.e., tangibility, intangibility, and their legal consequences: The core distinguish between digital and physical evidence is their inherent nature: digital evidence is intangible, can be tampered, altered easily, while physical evidence has a material form and relies on its tangible presence and the established procedures regarding its handling to maintain its authenticity, this distinction forms all the subsequent aspects of evidentiary handling and admissibility under the BSA and BNSS. Whilst both kinds of evidence must be relevant and reliable to be admissible, the methodologies for proving them reliable differ significantly.[22]

Collection and Preservation: Different Methodologies and Challenges

Physical Evidence: (Collection and Preservation under BNSS)-

Collection and preservation of physical evidence at a crime scene demands strict adherence to the procedures established by the statutes (BNSS, BSA) to maintain the authenticity of the evidence collected

Key Procedural Steps-

[22] Indian Express, 'Why Sc Has Laid Down Guidelines For The Management Of Dna Evidence' (The Indian Express, 19 July 2025) [19]

Crime scene management: According to Locard's Exchange principle: - "Every individual who enters or leaves the crime scene will contribute or remove material; thus, it's imperative to seal the area as soon as possible to prevent contamination, tampering of evidence.[23]

Documentation: A "walk-through" is conducted for the crime scene for initial documentation to identify 'Fragile or Perishable evidence 'this is preliminary documentation which includes photos(long-range, medium range, close-up with scale), videos, notes, detailed sketches of the scene and observation of scene conditions (e.g. Lights, exits, entries, doors windows, Odors, temperature, etc)[24]

Search Methodologies

- Wheel / Ray method for small circular scenes
- Spiral method for outdoor scenes
- Zone method for scenes where the area is divided into quadrants[25]

Packaging: The BNSS mandates that to protect the evidence from cross contamination and tampering it must be secured in containers at the crime scene itself, additionally the BNSS also provided for procedures such as each article (a potential evidence) must be packed separately labelled with the essential information such as FIR number, Date, IO's name, Police station, No, kind of articles, state, and such container must be duly signed by the IO.

Biological Evidences: Biological evidences are considered to be very sensitive, perishable, and fragile, hence collection of such evidences must be done by a trained personnel, who is well equipped and immediately such samples must be sealed in tamper proof containers with a clear labelling with relevant information, and must be immediately transported to the designated forensic labs within 48 hours after collection, furthermore proviso also state that storage of such samples must be done as such to prevent degradation.[26]

[23] Richard Saferstein, *Forensic Science: From The Crime Scene To The Crime Lab* (3rd Edn, Pearson Prentice Hall 2013) 45
[24] MHA, 'Investigating Officers' [21] <Www.Mha.Gov.In>
[25] LIFS, 'Forensic Science Crime Scene Investigation Complete Details' [20]
[26] LIFS, 'Forensic Science Crime Scene Investigation Complete Details' [20]

Role of forensic experts as per BNSS: The BNSS mandates under SECTION 176(3)(b)[27], for the forensic investigation for offences punishable with 7 years of imprisonment or more, i.e., the forensic experts are required to visit the crime scene to collect forensic evidence and additionally must record the entire process of forensic investigation using mobile phones or other electronic devices capable of recording. This represents a significant push towards professionalising and standardising physical evidence collection, which addresses the historical concerns about potential tampering of physical evidence. This shift from providing mere guidelines to making it statutorily mandatory ensures improved and increased accountability through transparency of the investigation.

Digital Evidence (Collection and Preservation Under BNSS And BSA): The collection and preservation of digital evidence brings forth unique challenges. Due to its intangible nature, it can be easily tampered with, overwritten, lost, deleted, altered, and erased; hence, it imposes the need to bring forth specialised techniques to maintain the authenticity of the digital record.

"Live" vs. "Static" Data Acquisition: This method involves imaging a running system to capture the volatile information (such as what programs are open, who's connected to the internet, what's in the computer's memory(RAM), etc) that would disappear if the system were turned off. It is crucial to capture such evidences which constantly keeps on changing, and in doing so one must be very careful to prevent the accidental change or damage or even destroying of the data that can be used as evidence, for so it is imperative not to shut down the system until the whole data is been collected, one can also note the system ate, time, command history, and dumping RAM into a sterile removable storage device.[28]

Static Data Acquisition: This method refers to the extraction of non-volatile data from storage media like hard drives, USB drives and smartphones, etc. there are many methods for the collection of this information, but one needs to still need to duplicate the original data and perform the investigation on the duplicate instead of the original data to keep it safe and as a backup.[29]

Dead/ Offline Acquisition: This method involves powering down the system to remove the hard disk to image it. This method is used to preserve the file data and prevent further changes

[27] Bharatiya Nagarik Suraksha Sanhita 2023,S 176(3)(B)
[28] Info-Savvy, 'Live Data Acquisition' Https://Info-Savvy.Com/Live-Data-Acquisition/ Accessed 18 July 2025
[29] Info-Savvy, 'Understand Static Data Acquisition' Https://Info-Savvy.Com/Understand-Static-Data-Acquisition/ Accessed 18 July 2025

during the imaging. Collecting data from cloud storage or remote devices presents unique jurisdictional and logistical challenges.[30]

Comparison: Digital evidence imposes complex challenges in the initial collection and preservation of data. The professionalism and technical knowledge required for the collection of digital evidence are significantly more complex than those for physical evidence, which relies on manual protocols.

AUTHENTICATION OF EVIDENCE (UNDER BSA)

Physical Evidence (Under BSA): Physical evidence's admissibility under BSA's proviso is as: section 56[31] i.e. the contents of the evidence must be proved either by primary which refers to be the original document itself(considered to be the best proof) or secondary evidence which refers to include copies, certified extracts, etc when the original is unavailable under legitimate conditions, additionally the section 67-73[32] of the BSA governs the proof of execution and authentication of documents. Furthermore, certain documents such as government records, official publications, certified copies of legal documents, maps, surveys by government authorities, newspapers, and powers of attorney exercised before the notary carry a presumption of authenticity, though these presumptions are rebuttable.

Digital Evidence (Under BSA): For the admissibility of electronic records, the BSA introduces a comprehensive framework. Section 63 of BSA equivalent to the section 65 of IEA, is a pivotal section which defines "computer output" as admissible evidence without requiring the original record, such outputs are deemed equivalent to original documents if specific conditions (such as regular use of the device, regular feeding of information, proper operation of device.)are met, additionally it must be signed by both the person in charge of the computer and an expert, which must include the harsh value of the electronic record before printing it. Forensic expert testimony also heavily influences the authentication of the digital record as evidence. The *"original" dilemma* under BSA section 57, the classification of digital records as primary evidence in certain conditions, fundamentally shifts the traditional 'original' concept. This contrasts with the physical "best evidence rule" for original documents, where

[30] Scribd, 'Live Vs Dead Computer Forensic Image Acquisition' Https://Www.Scribd.Com/Document/582427113/Ijcsit2017080331 Accessed 18 July 2025
[31] Bharatiya Sakshya Adhiniyam 2023, S 56
[32] Bharatiya Sakshya Adhiniyam 2023, S 67- S 73

the physical documents itself is paramount. There is an inherent ease of digital manipulation, which imposes the need to have a complex technical step to prevent tampering.

Comparison: Authenticity of digital records as evidence always requires specialised expertise and compliance with the specific provisos of the BSA, such as section 63 or proof of "proper custody" under section 57, which usually does not apply in most physical evidence, which relies on direct observation and established scientific protocols.

CHAIN OF CUSTODY: SAME PRINCIPLE, DIFFERET OPERATIONALISATION UNDER BNSS

To ensure the authenticity and integrity, and verifiability of both the physical and digital evidence, maintaining a chain of custody is pivotal.

Physical Evidence - The Traditional Chain of Custody: A documented sequence of possession, transfer, and storage from the crime scene to the courtroom, i.e., to lodge in at each level of handling and transfer with a counter signature at each level, along with a clear reason for the transfer, this rigorous procedure ensures prevention of evidence tampering at any stage. Many provisions of the BNSS for police duties (i.e., relating to case diaries, panchnamas, seizure memos, etc)[33]

Digital Evidence: Chain of Custody: Chain of custody for the digital evidence involves the logging of every access, copy, change, handling of files and devices, etc Some challenges, such as improper shutdown leading to evidence getting altered or deleted, robust security systems, comprehensive logs, and encryption, are crucial for evidence protection. Hash values play a critical role, serving as unique digital fingerprints that verify the integrity and detect tampering. Along with the BNSS mandates, which strengthen the chain of custody of digital records. [34]

Expert Testimony: While experts enhance the probative value of physical evidence as under section 45 of BSA, these testimonies are often prerequisites for the very acceptance and understanding of the digital evidence (as under section 46 of BSA and section 79A of IT Act,

[33] Satya Prakash,"Supreme Court Issues Guidelines For Collection, Preservation, Processing Of Dna/ Forensic Evidence.",Tribune News Service, Updated 116july,2025 Ist
[34] Standard Operating Procedure(Sop) For Audio-Visual Recording Of Scene Of Crime, Bureau Of Police Research & Development <bprd.nic.in>

which accompanies it), by the court. These technical complexities and inherent vulnerabilities of digital data make experts' testimony pivotal for admissibility.

CONCLUSION OF COMPARISON

Although the main goal of reaching justice is the same, the inherent intangible and volatile nature of digital evidence puts forth a fundamentally different set of technical and procedural requirements when compared to physical evidence.

EVIDENTIARY CHALLENGES AND IMPLEMENTATIONAL GAPS UNDER THE NEW LAWS

Although the new laws, such as BSA, BNSS, aim to modernise the legal procedures, there remain significant challenges that persist in the practical application of these provisions, especially concerning digital evidence.

Challenges of Authentication and Integrity of Digital Evidence The Truth, The Whole

Truth, and The Digital Truth: Trying to determine if a digital photo is real or fake, or where an online message came from, is a big challenge when it comes to verifying digital evidence. Law enforcement often lacks the specialised training and consistent procedures needed to handle digital crime scenes. This can lead to crucial evidence being mishandled right from the start. It's hard to trace the true origin of digital data, especially from anonymous communications or shady online spaces. Additionally, the massive amount of digital data we generate daily from apps and devices overwhelms police agencies, causing huge backlogs. And with AI-generated content like deepfakes becoming more advanced, differentiating between real and fake is a new challenge that the BSA hasn't fully addressed.

Getting All Our Ducks In A Digital Row - Collecting, Preserving, And Presenting Digital Evidence Is Not A Smooth Process: It's like trying to get different teams, such as police, forensic labs, prosecutors, and judges, to work together effectively when they have different approaches. A lack of coordination leads to important information getting trapped in separate digital silos, making it difficult to build a complete picture. Moreover, many departments don't have funds for the latest tools and equipment and the ongoing training needed to tackle digital crime, especially in smaller towns. This leads to delays and a shortage of experts. Also, there's a communication gap between the technical experts and legal practitioners, including judges, to understand complex digital evidence.

Privacy vs. Pursuit of Justice - A Tightrope Walk: This is a big challenge: balancing our right to privacy with the state's need to collect digital evidence for investigations. The new Digital Personal Data Protection Act is a step towards protecting personal data, but it adds another layer of complexity for law enforcement. E.g., when a phone is encrypted by default, it's great for privacy, but it makes it very difficult for the police to access the evidence. Courts are constantly considering the balance between surveillance powers and privacy rights, and law enforcement must be careful to maintain public trust.[35]

The Bench's Digital Learning Curve: Judges also face a steep learning curve. They are tasked with interpreting new legal concepts introduced by the BSA and BNSS, especially those related to digital evidence. Many judges lack the deep technical know ledge needed to fully understand digital evidence or to effectively question expert witnesses. This can further lead to longer trials as disputes over digital evidence continue. There's also a risk that different courts may interpret these new laws differently until the Hon'ble SC provides clear guidance, leading to a patchwork of rulings.

A Fair Fight in the Digital Courtroom: Finally, for defence attorneys and those accused of crimes, the playing field isn't always level. It's often hard for the defence to afford their digital forensic experts or to independently analyse digital evidence presented by the prosecution. This makes it extremely difficult for them to challenge the technical validity of the state's digital evidence. This imbalance in digital capabilities raises serious concerns about fairness and due process, especially when one side can't properly examine the complex digital evidence against them.
It's clear that while the new laws are a step forward, there's still a lot of work to be done to ensure they function smoothly and fairly in our increasingly digital world.[36]

[35] Europarl, 'Digital Personal Data Protection Act 2023 Impact On Police Digital Evidence Collection' (Europarl, 2025) Accessed 19 July 2025
[36] Major Cities Chiefs Association, 'Mcca Digital Evidence White Paper' (Mcca, October 2023) Accessed 19 July 2025
Researchgate, 'Digital Forensic Science And Evidentiary Standards In The Bharatiya Sakshya Adhiniyam (Bsa) 2023: A Legal Examination Of Admissibility' (Researchgate, 2025) Accessed 19 July 2025
Vidizmo, 'Handling Digital Evidence' [Https://Vidizmo.Ai/Blog/Handling-Digital-Evidence] Accessed 19 July 2025

CONCLUSION AND RECOMMENDATIONS: NAVIGATING DIGITAL JUSTICE IN INDIA

Reaffirming The Digital Leap with Caveats: India's new BSA AND BNSS denote significant steps towards modernising the legal system, clearly acknowledging digital evidence as primary. However, the lack of clear guidelines, inconsistent judicial understanding, and the complex nature of digital evidence mean there are still major challenges. These issues require urgent updates to procedures, specialised training, and clearer laws to ensure justice is delivered fairly and effectively in the digital world.

Key Takeaways from The Digital Shift: The BSA and BNSS have changed how India's legal system works by including digital evidence and using technology in investigations. Still, many problems remain. Digital data can be easily changed or lost, forensic resources are limited, there are not enough skilled experts in digital forensics, and there's a constant struggle between protecting privacy and allowing investigations. The success of these changes depends on consistent use and clear judicial guidance, especially around BSA sections 57 and 63.

The Stakes: Credibility and Trust In The Digital Age: Managing digital evidence properly is essential for maintaining public confidence in India's criminal justice system. As society becomes more digital, the legal system must be able to handle this type of evidence to protect basic rights, ensure fair trials, and fight modern crimes. How well these reforms are implemented will determine India's ability to provide justice in the digital era.

A ROADMAP FOR DIGITAL JUSTICE REFORM

To fully benefit from these legal changes, focused efforts are needed across several key areas:

Legislative and Policy Refinements-

Clarify BSA Provisions: Update the BSA to remove confusion, especially around how Section 57 (digital evidence) and Section 63 (certification requirement) work together.

Deal with New Digital Evidence: Create specific rules for handling new types of evidence, such as blockchain records, AI-generated content like deepfakes, and IoT data.

Align with DPDP Act: Offer clear legal guidance on how the DPDP Act, 2023, interacts with law enforcement's ability to seize data.

Develop a National Digital Forensics Policy: Create a comprehensive policy that sets standards, allocates resources, and promotes collaboration between different agencies.

Empowering Law Enforcement (under BNSS)

Mandatory Advanced Training: Ensure all officers, first responders, and prosecutors get ongoing training in digital forensics.

Follow International Standards: Enforce national SOPs for digital evidence that match global forensic standards.

Invest in Infrastructure: Provide long-term funding for modern digital forensic labs, tools, and software.

Strengthen Cybercrime Units: Expand specialised cybercrime teams with advanced skills and multi-disciplinary support.

Enhancing Judicial Competence

Regular Judicial Training: Offer frequent, mandatory training for judges on digital evidence rules, cyber laws, and practical forensics.

Manage Expert Witnesses: Develop strong guidelines for accrediting and managing digital forensic experts, possibly through a central system.

Use Technology in Courts: Further integrate digital tools in courtrooms and explore the creation of "cyber benches" for complex digital cases.

Ensuring Equitable Access to Justice

Legal Aid for Digital Forensics: Provide government-funded digital forensic experts for people who can’t afford them, so they can properly challenge prosecution evidence.

Public Awareness Campaigns: Educate the public on digital evidence and cyber safety to promote understanding and protection.

Enhanced International Cooperation

Streamline MLATs: Make Mutual Legal Assistance Treaties faster and more efficient for accessing digital evidence across borders.

Participate in International Agreements: Actively join and consider ratifying international cybercrime agreements like the Budapest Convention.

FUTURE OUTLOOK AND RESEARCH

The path to a strong digital justice system in India has just started. While legal reforms are an important first step, their success depends on ongoing efforts to solve challenges related to infrastructure, staffing, and how laws are interpreted. Future research should explore how AI affects evidence, the difficulties of blockchain and IoT forensics, and the ethical issues of new digital technologies and surveillance under these changing laws.

APPENDIX

This appendix provides a detailed observation of the survey conducted to gather the differences in digital evidence within the Indian legal justice system to gather insight into the attitude, especially in the context of the newly implemented Bharatiya Sakshya Adhikar (BSA), 2024. It is divided into two main segments. Collage reactions.

Appendix A: Survey Questions

This section contains the precise questions asked of the participants of the survey.

What Is Your Primary Professional Role?

- Law Aspirant
- Law Student (UG/PG)
- Advocate/Practising Lawyer
- Academic Researcher (Law)
- Digital Forensic Expert
- Retired faculty

How Many Years Of Experience Do You Have In The Legal Justice System?

- Less than 1 year
- 1-3 years
- 4-7 years
- 8-15 years
- More than 15 years
- No experience

In Which State/ Region Do You Primarily Practice or Reside?

- Open-ended text response

AWARENESS AND IMPACT OF THE BSA'S IMPLEMENTATION

Before this survey, were you fully aware that the Indian Evidence Act, 1872, was replaced by the Bharatiya Sakshya Adhiniyam (BSA), w.e.f. July 1st, 2024?

- Yes, fully aware
- Yes, vaguely aware
- No, I was not aware

How familiar are you with specific provisions of the BSA, 2024, about digital evidence (e.g., Section 2(1)(d), Section 57, Section 63)?

Scale of 1 to 5 (1 = Not familiar at all, 5 = Very familiar)

Do you believe the BSA, 2024, significantly improves the framework for admitting digital evidence compared to that of the Indian Evidence Act, 1872?

- Yes, significantly improves.
- Slightly improves
- No significant changes

- Makes it more complicated
- Unsure

ADMISSIBILITY AND PRACTICAL CHALLENGES FOR DIGITAL EVIDENCE

In your experience, what type of digital evidence is most frequently encountered in criminal trials?

- Call data records (CDRs)
- Location Data
- SMS/ Messaging App Data (WhatsApp, Telegram, etc.)
- Social Media Posts/Profile (Instagram, Twitter, etc.)
- CCTV/Video Surveillance Footage
- Computer/Laptop Data (Browse History, IP Logs, Website Data)
- Banking Transaction Data
- Being honest depends on the case and its nature. In one of my cases, it was more based on call and location.

How challenging is it, in practice, to obtain the necessary certificate under section 63(4) of BSA (corresponding to Section 65 B(4) of the Indian Evidence Act, 1872) for digital evidence?

Scale of 1 to 5 (1 = Not challenging at all, 5 = Very challenging)

What is the biggest hurdle in proving the authenticity and integrity of digital evidence in court?

- Difficulty in obtaining section 63(4) of BSA, certificate
- Lack of proper chain of custody documentation
- Concerns about tampering or manipulation

- Insufficient technical expertise of legal professionals
- Lack of standardised procedures (forensic, etc.)
- Resistance from the third-party service providers (e.g., Intermediaries, companies, etc.)

Do you believe the BSA's classification of certain digital records as "primary evidence" (Section 57, explanations 4-7) will significantly reduce the reliance on section 63 certificates?

- Yes, significantly
- Somewhat
- No, the certificate will still be widely required
- Unsure

How would you rate the current state of digital Forensic capabilities (e.g., labs, trained personnel) available to law enforcement in India?

Scale of 1 to 5 (1 = Very poor, 5 = Excellent)

COMPARISON WITH PHYSICAL EVIDENCE & WAY FORWARD

In your opinion, which type of evidence (digital/physical) is generally more challenging to collect and preserve without compromising its integrity?

- Digital
- Physical
- Both are equally challenging
- Unsure

Do you think judicial officers and legal professionals possess adequate technical understanding to effectively deal with complex digital evidence?

- Yes, generally

- Some do, but there's a significant gap
- No, there is a widespread lack of understanding
- Unsure

What is the most critical reform needed to improve the handling and admissibility of digital evidence in Indian criminal trials?

- Comprehensive training for law enforcement on digital forensics
- Increased Funding for Digital Forensic Infrastructure and Labs
- Development of standardised national protocols for digital evidence collection
- Enhanced international cooperation for cross-border digital evidence

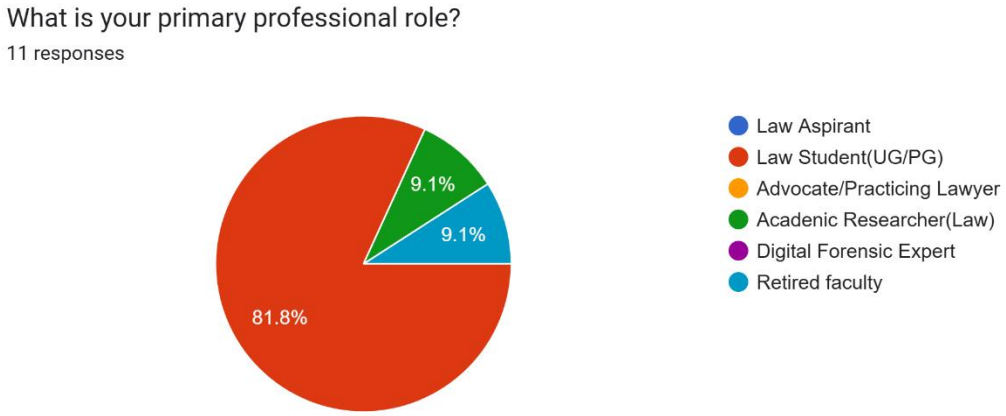
Any additional comments or suggestions regarding Digital evidence in Indian criminal trials?

Open-ended text response

APPENDIX B

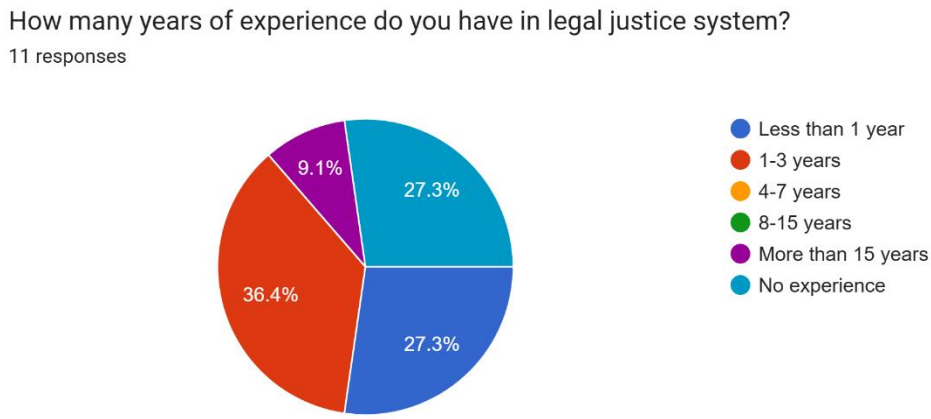
This analysis summarises the responses from 11 participants on various aspects of digital evidence, the impact of the Bharatiya Sakshya Adhiniyam (BSA), 2024, and challenges in its handling and admissibility in Indian criminal trials/.

Primary Professional Role



Overview: The overwhelming majority of respondents are students (UG/PG) of the law. This indicates that insight mainly reflects the perspective of those who are currently immersed in legal education, possibly with theoretical knowledge of recent legal development. Despite being valuable, his reactions may lack the experience of the practical court of experienced legal physicians. The inclusion of an academic researcher and a retired faculty member gives some diversity, but the reaction does not significantly change the student-centric nature.

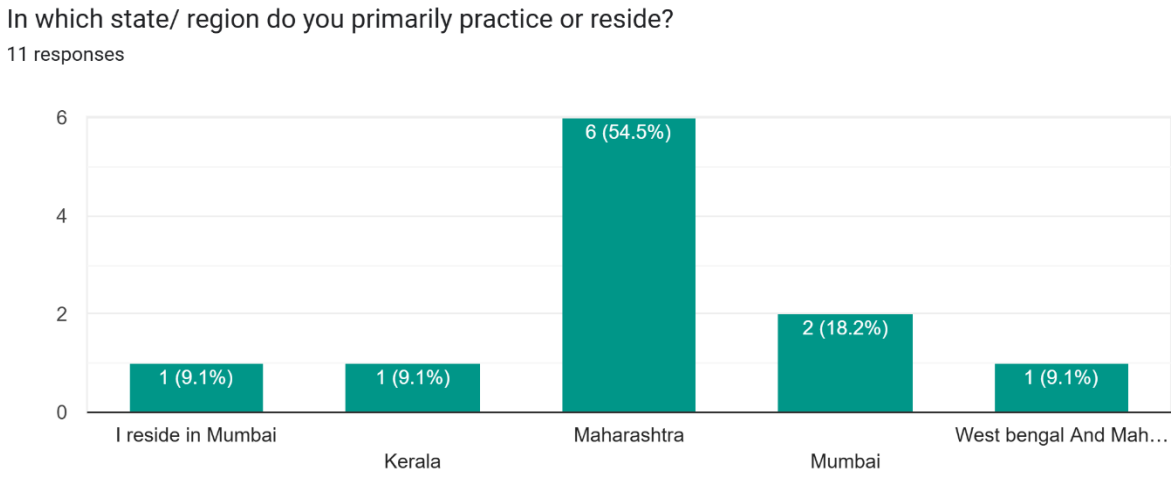
How Many Years Of Experience Do You Have In The Legal Justice System?



Overview: Data shows that 63.7% of respondents have very limited or no direct experience in the legal justice system (or no experience less than 3 years). This confirms the observation about the prevalence of students of the law in the survey. Although they are well aware of recent legislative changes such as BSA, their answer and digital evidence may be more based

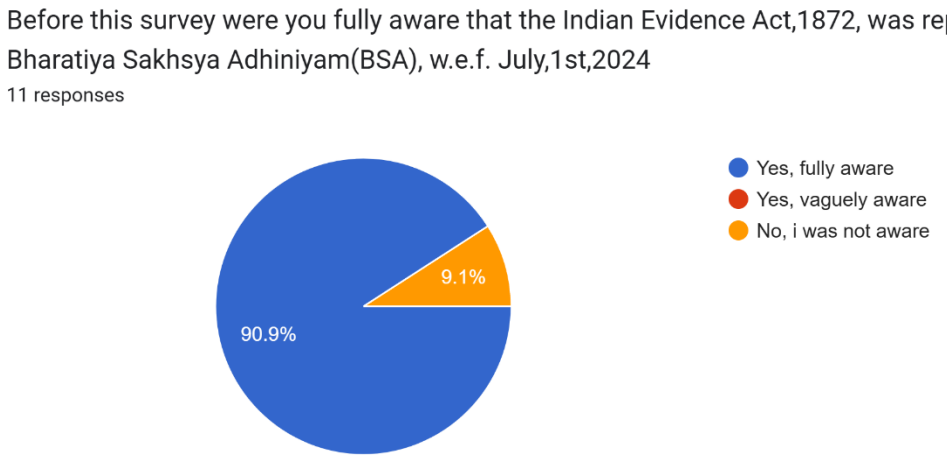
on academic understanding of the real-world implications of the real-world related to practical challenges. The possibility of a single defendant, an educational researcher, or retired faculty with an experience of "more than 15 years", provides a contrast, a more experienced perspective.

In Which State/ Region Do You Primarily Practice Or Reside?



Overview: Survey Pool Maharashtra, especially in Mumbai, is very focused on Mumbai, accounting for 81.8% reactions. This geographical concentration means that the findings can be more reflective of the legal scenario and can withstand challenges related to digital evidence within this specific region, rather than a pan-Indian representation. While Mumbai is an important legal centre, experiences in other states or rural areas may vary greatly.

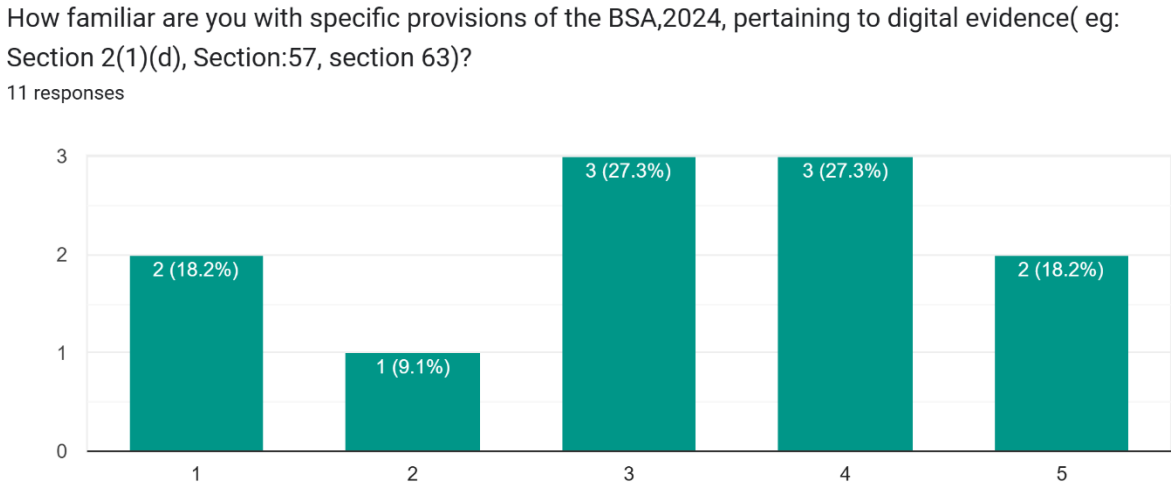
Before This Survey, Were You Fully Aware That The Indian Evidence Act, 1872, Was Replaced



By The Bharatiya Sakhsya Adhiniyam (Bsa), W.E.F. July, 1st, 2024

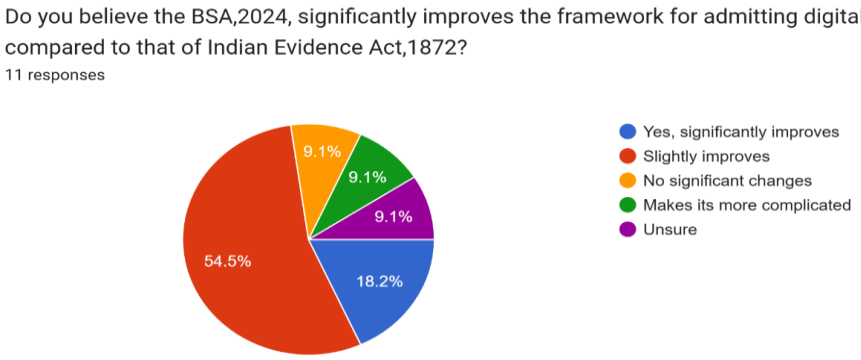
Overview: The survey reveals an extraordinarily high level of awareness about the replacement of the Indian Evidence Act, 1872, which has been done by the Indian Witness Adhiam (BSA), effective since July 1, 2024. This suggests the success of information about this important legislative change within the legal community, especially among the students of the law, who are among the new generation.

How Familiar Are You with Specific Provisions of the BSA, 2024, About Digital Evidence (Eg, Section 2(1)(D), Section 57, Section 63)?



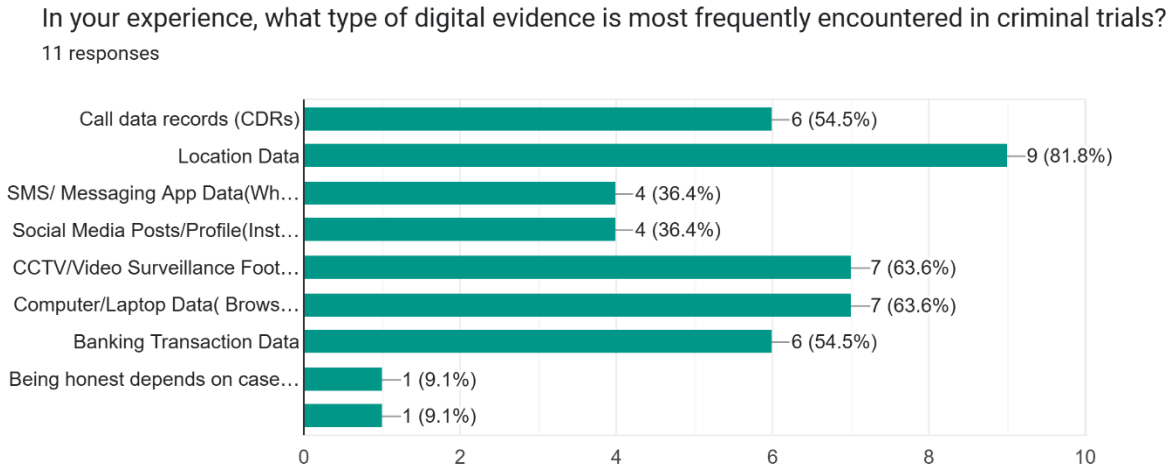
Overview: While general awareness about the enactment of BSA is higher, familiarity with its specific provisions related to digital evidence is more diverse. Broadly, half of the respondents (45.5% scoring 4 or 5) consider themselves highly familiar, which is positive. However, a significant part (27.3% scoring 1 or 2) indicates low familiarity, and another 27.3% is mildly familiar (Scoring 3). This shows that while the new law is known, its complex details, especially for people related to digital evidence, still need intensive study and understanding throughout the board.

Do You Believe The BSA, 2024, Significantly Improves The Framework For Admitting Digital Evidence Compared To That Of The Indian Evidence Act,1872?



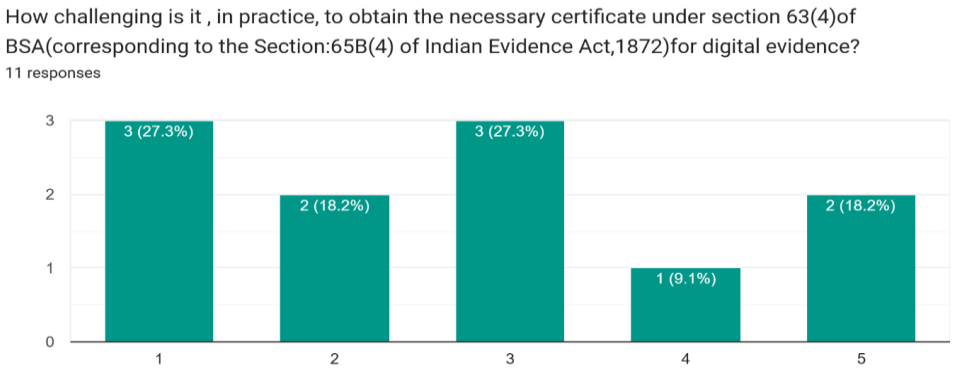
Overview: The main feeling is that BSA provides only a slight improvement (54.5%) in the framework to accept digital evidence rather than a revolutionary change. Only one minority (18.2%) considers a "significant improvement". This indicates a vigilant optimism or lack of strong trust that the BSA can completely resolve the complex challenges of digital evidence. The fact is that some believe that it complicates cases or does not make any significant changes, which suggests doubts about the influence of the real world.

In Your Experience, What Type Of Digital Evidence Is Most Frequently Encountered In Criminal Trials?



Overview: The survey recognises location data, CCTV/video surveillance footage, and computer/laptop data as the most frequently faced forms of digital evidence. This highlights the wide role of monitoring and digital footprints in modern criminal probes. Call data records (CDRs) and banking transactions are also highly relevant. SMS/messaging app and low frequency of social media data may suggest challenges in their collection or acceptance, despite their general use in personal communication.

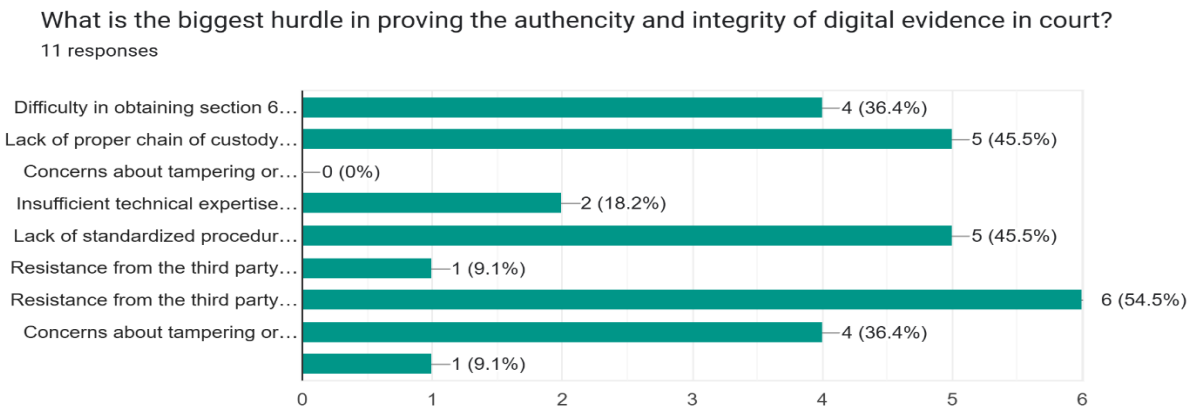
How Challenging Is It, In Practice, To Obtain The Necessary Certificate Under Section 63(4) Of BSA (Corresponding To Section 65B(4) Of The Indian Evidence Act,1872)For Digital Evidence?



Overview: Section 63 (4) Opinions about the difficulty of obtaining certificates are highly fragmented. While a vital part (27.3%) does not seem challenging at all, a similar part (18.2%in 5) seems very challenging. This inequality may reflect the difference in experience, the nature

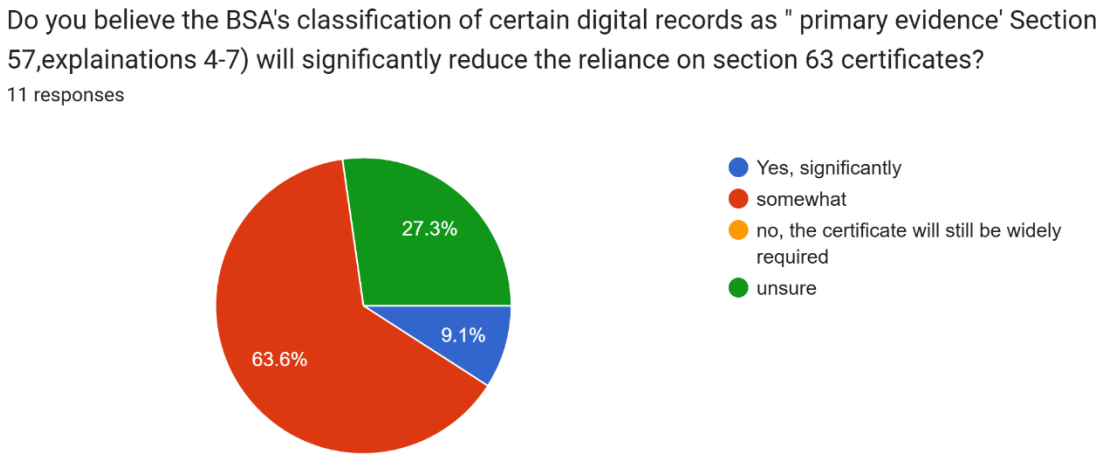
of specific cases, or regional variations in legal practice. The fact that a combined 54.6% has given it a 3 or higher status suggests that for many people, it is a notable practical barrier.

What Is The Biggest Hurdle In Proving The Authenticity And Integrity Of Digital Evidence In Court?



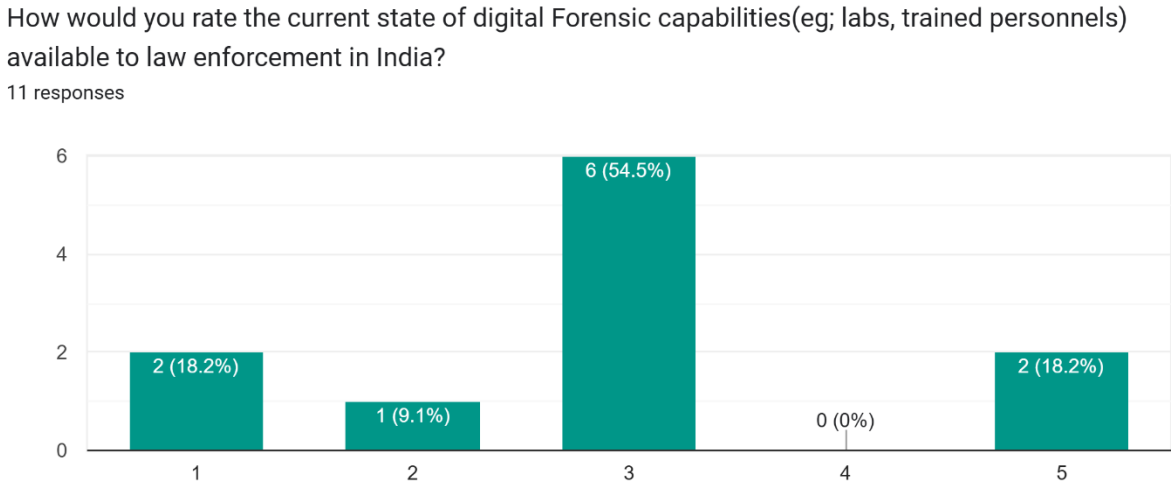
Overview: The most important obstacles identified are resistance from third-party service providers, together with the lack of a proper range of custody documentation and the absence of standardised forensic processes. This only indicates systemic issues beyond legal provisions - a strong, similar protocol requirement for cooperation and evidence handling with private institutions. Concerns about molestation and the difficulty of obtaining certificates also remain important challenges.

Do You Believe The BSA'S Classification Of Certain Digital Records As " Primary Evidence' Section 57, Explanations 4-7) Will Significantly Reduce The Reliance On Section 63 Certificates?



Overview: A major majority (63.6%) believes that the classification of BSA of some digital records as "primary evidence" will only reduce the dependence on "some extent" to some extent section 63 certificates. This suggests that during a positive step, it is not seen as a silver bullet that will eliminate the requirement for the certificate. The uncertainty expressed by 27.3% indicates that the practical implications of this provision have not yet been fully understood or felt.

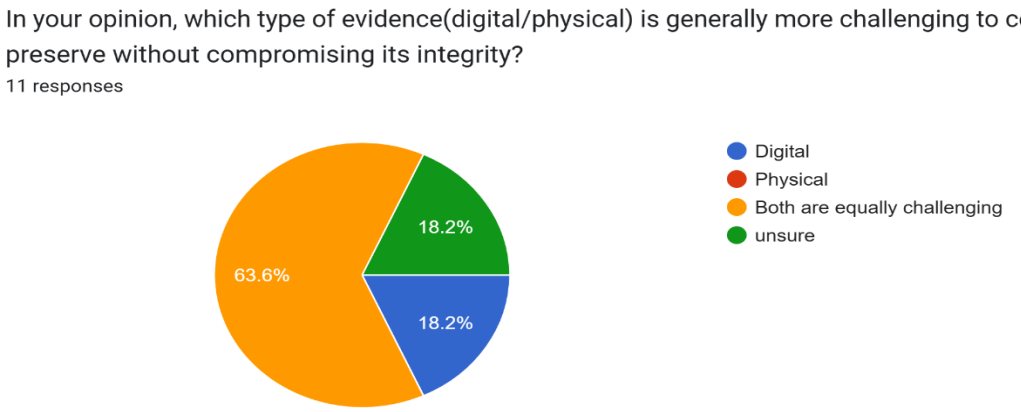
How Would You Rate The Current State Of Digital Forensic Capabilities(Eg, Labs, Trained Personnel) Available To Law Enforcement In India?



Overview: The average perception of digital forensic capabilities among law enforcement in India is moderate (3 rated by 54.5% of respondents). While some rate it as very poor, a similar

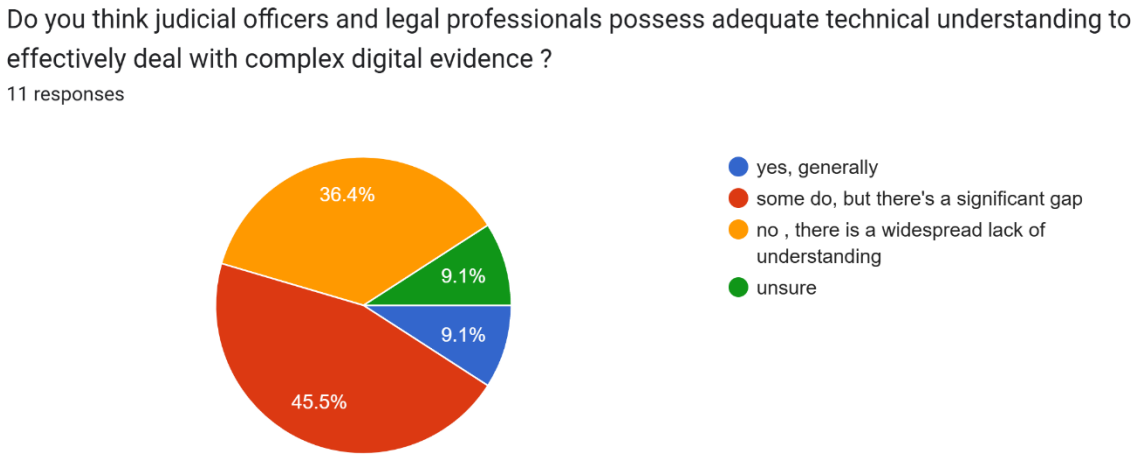
number rate it as excellent, which reflects potential regional inequalities or different experiences. However, the majority of scenes suggest that there is considerable space to improve infrastructure and reference to trained personnel to adequately handle the increasing volume and complexity of digital evidence.

In Your Opinion, Which Type Of Evidence (Digital/Physical) Is Generally More Challenging To Collect And Preserve Without Compromising Its Integrity?



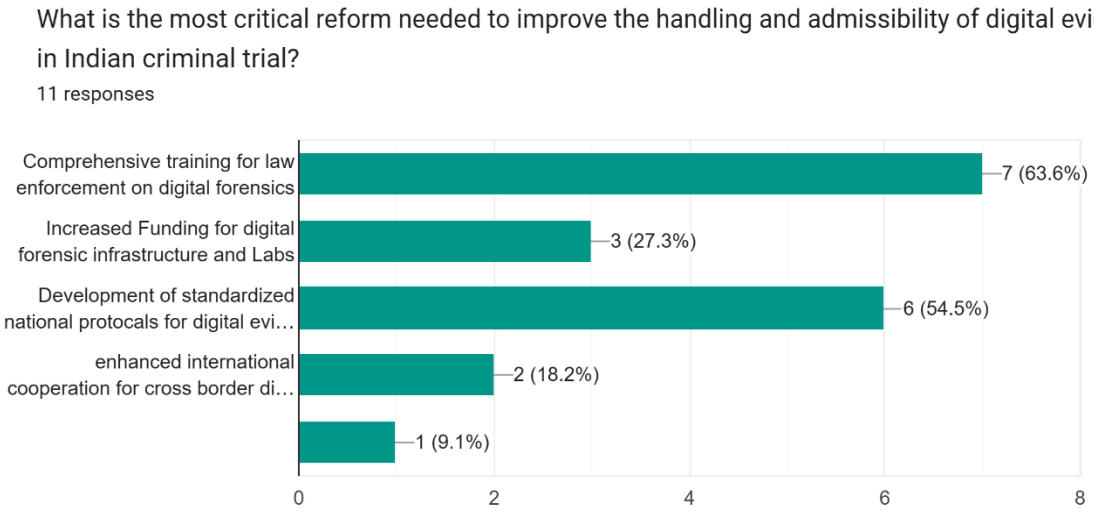
Overview: The prevailing opinion is that both digital and physical evidence present comparable challenges in the context of preservation of collection and integrity. This indicates a maturity in understanding that digital evidence, despite unique characteristics, is not naturally more difficult than physical evidence, provided that the proper protocol is followed. This suggests that issues lie more in the application of appropriate procedures than in the underlying nature of evidence.

Do You Think Judicial Officers And Legal Professionals Possess Adequate Technical Understanding To Effectively Deal With Complex Digital Evidence?



Overview: A Stark majority (81.9%) indicates a significant decrease in technical understanding of judicial authorities and legal professionals when it comes to complex digital evidence. This is an important observation, as even strong laws and forensic capabilities can be reduced if there is a lack of necessary technical literacy in the interpretation and prosecuting bodies. This difference may lead to misinterpretation, unfair acceptance decisions, and a common obstacle to justice in matters related to digital evidence.

What Is The Most Critical Reform Needed To Improve The Handling And Admissibility Of Digital Evidence In Indian Criminal Trials?



Overview: The survey highlights two paramount requirements: extensive training for law enforcement on digital forensics and the development of a standardised national protocol for digital evidence collection. These two reforms are seen as a foundation to improve the entire ecosystem of digital evidence handling, from the seizure to the presentation in court. Increased funding and international cooperation are also recognised as important, but secondary to these primary training and standardisation initiatives.

Any Additional Comments Or Suggestions Regarding Digital Evidence In Indian Criminal Trials?

Overview: Qualitative response underlines the practical concerns and aspirations of the legal community about digital evidence. There is a strong call for this.

Technological Progress In Proving Authenticity: This reflects the ongoing challenge to establish the credibility of digital evidence in the court.

More Competent Law for Evidence Acquisition: Suggests that the current legal mechanism may still be insufficient or cumbersome to obtain digital data.

AI-Penked/Active Legal Framework For Modified Evidence: This AI indicates carrying forward further concerns about emerging technologies to manipulate or make evidence, which requires immediate legal reactions.

Emphasis on Procedural Reforms And Infrastructure: Calls for easy access to forensic experts, a national structure (eg NIST), compulsory series-c-kasty protocols, and a continuous training system for police and judiciary strengthenthe need for systemic, practical reforms.

Public Awareness: This broad suggestion indicates the need for public understanding of the legal implications of digital evidence, perhaps to promote better cooperation or responsible digital behaviour.