

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA)*.

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

**Copyright © International Journal for Legal Research & Analysis.
All rights reserved.**

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ADMISSIBILITY AND EVIDENTIARY VALUE OF AI-GENERATED DIGITAL EVIDENCE UNDER THE BHARATIYA NAGARIK SURAKSHA SANHITA, 2023

AUTHORED BY - SHAISTA NAAZ

Assistant Professor

Bhishma Narain Singh Law College Medininagar, Palamu, Jharkhand, India

Abstract

The Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023 and Bharatiya Sakshya Adhiniyam (BSA), 2023 are the two most important changes in the Criminal Justice System of India by way of statutes. But the rise of artificial intelligence (AI)-created content and deepfakes poses a major evidentiary issue that threatens to throw this balance off. This paper aims to assess the admissibility and probative value of AI-generated digital evidence within the framework of the BNSS and BSA. According to the analysis of Section 63 of the BSA, the certification system and reliance on cryptographic hash values are primarily used to ensure data integrity after the media have been created, but are not sufficient to stop the production of fake media at the time of creation. In addition, the operational challenges of the BNSS procedures, including collection and mandatory forensic collection, are significant because of the absence of an institutional infrastructure. The paper proposes moving from statutory admissibility to a reliability standard for judicial assessment, which should involve transparency of the algorithms, independent corroboration, and specialized forensic assessment, to ensure constitutional guarantees of a fair trial.

Keywords: Bharatiya Nagarik Suraksha Sanhita 2023, Bharatiya Sakshya Adhiniyam 2023, AI-generated evidence, Deepfakes, Digital forensics, Admissibility, Cryptographic hash values, Probative value, Chain of custody, Algorithmic transparency.

The Evolution of Evidentiary Jurisprudence in the Digital Era

The radical overhaul of the Indian criminal justice system, embodied in the Bharatiya Nagarik Suraksha Sanhita (BNSS), 2023, and the Bharatiya Sakshya Adhiniyam (BSA), 2023, marks a radical shift away from the colonial legal frameworks. To fill the historic gap between the old

and the new law, the Indian legislature has tried to fill gaps in the Code of Criminal Procedure, 1973, and Indian Evidence Act, 1872 (Verma, 2025)¹. The modern criminal trial has changed radically from that of the past; it is not solely dependent on physical evidence or the faulty human memory of the witness. Rather, the modern adjudication is far more tied to an elaborate tangle of electronic footprints, logs from servers, metadata of communications, and digital media. This statutory change brings electronic records to the forefront from a lowly status of secondary evidence, to the realm of primary evidence, compelling the criminal investigation and judicial evaluation to be technology-centric (Kumar, Sakshi, & Medhi, 2026)². As legal scholars universally acknowledge, this is a part of the legislative evolution needed to modernize how the law treats digital evidence, yet at the same time it adds a new level of complexity to the questions of authenticity, integrity, and final probative value of digital evidence in courts. Such complexity is now being complicated in an unprecedented way by the advent of generative artificial intelligence, advanced machine learning algorithms and synthetic media known as deepfakes, in the legal and technical literature. The high-end technologies have the potential to generate hyper-realistic AV content that could manipulate and mimic the reality, disrupting the epistemological assumption, on which the entire criminal justice system is based (Mishra & Shukla, 2026)³. The BNSS and the BSA provide a detailed and interlocking model of statute which regulates the seizure, preservation and presentation of digital evidence in this fast-changing environment. The legal system assumes that strict adherence to procedures combined with sophisticated cryptographic verification mechanisms, like hashes, will be enough to guarantee that the truth-finding process will not be manipulated through digital means (Gupta, 2026)⁴. The underlying premise of these new laws, however, is largely based on traditional forms of electronic evidence, including unaltered Closed Circuit Television (CCTV) footage, authentic Call Detail Records (CDR) and regular email communications. But with the rise of AI-powered content, this logic behind the legislation is completely turned on its head. A complex algorithm can combine a voice recording with another dialogue to create a new voice recording that appears as authentic as the original, and a video of a fake event can be made to look real by overlaying a live recording with computer-generated footage of the same event, so traditional techniques of verifying that a data transmission or data storage integrity has not been compromised are now dangerously out of date (Varshita, 2026)⁵. No longer can the central question of modern evidence law be whether a digital file was altered after it was created, but it must now be whether the event represented by the electronic file ever actually happened. This study thus comprehensively examines the admissibility requirements and the prima facie evidence of AI-generated digital evidence under the BNSS and BSA 2023,

and critically analyzes the conflict between statutory provisions, the evolving judicial understanding of AI-generated digital evidence, and the algorithmic nature of the medium.

Statutory Mandates and Procedural Restructuring under the BNSS, 2023

The Bharatiya Nagarik Suraksha Sanhita, 2023, essentially redefines the investigative duties of police, laying them down as a non-discretionary duty and not merely an option but a mandatory statute for police across the country to perform. The most impactful of the innovations in this procedural improvement is contained in Section 176(3) of the BNSS. This particular provision is a clear-cut requirement that the officer in charge of a police station should make sure that the crime scene is visited by a forensic expert who will collect forensic evidence in case of a crime punishable by seven years or more of jail time (Khan & Srivastava, 2026)⁶. In addition, the procedure for evidence gathering needs to be recorded on a cell phone or any type of other recognized electronic device and videotaped throughout. This is a radical change from the previous Section 157 of the CrPC which left it as a negative obligation for the State to ensure that scientific methodology is used from the beginning of every major criminal investigation. The clear intent of this provision is that it is meant to reduce the historic dependence on easily manipulated testimonial evidence and to build a verifiable, unfolding chain of custody from the original crime scene back to the courtroom floor.

This directive on digital documentation of search and seizure is complemented by Section 105 of BNSS, which mandates for all search and seizure operations, a mandatory audio video recording shall be made and shall be sent to the District Magistrate or Judicial Magistrate immediately. Likewise, video requirements are the same for general police searches done as part of an investigation (PRS Legislative Research, 2023)⁷. This procedural design is very carefully crafted to eliminate opaqueness and procedural arbitrariness inherent in police searches and seizures in India. The BNSS is meant to replace the old-fashioned methods of planting, tampering with, and overlooking evidence, by forcing law enforcement officials to record the discovery and preservation of physical and electronic evidence in a digital manner. In addition, s. 193(2)(i) of the BNSS explicitly imposes the chain-of-custody requirement on the statutory reporting framework by mandating police investigation reports to explicitly state the custody chronology of all seized electronic devices (Khan & Srivastava, 2026)⁶.

The BNSS term "audio-video electronic means" is defined in Section 2(1)(a) and finds its way through the entire procedural code. The technological integration is also seen in various processes relating to the formal arrest of persons, such as under Section 54; the recording of confessions and statements, under Section 183; the electronic service of summons, under

Sections 64 and 70; and the extension of judicial custody through electronic communication under Section 187 (PRS Legislative Research, 2023)⁷. Furthermore, section 530 of the BNSS marks a major change in that it explicitly provides that all trials, inquiries and proceedings under the code shall be conducted in electronic form.

Table 1: Doctrinal and Procedural Shifts Governing Evidence Collection and Administration.

Legal Feature or Procedural Provision	Code of Criminal Procedure, 1973 (Repealed Framework)	Bharatiya Nagarik Suraksha Sanhita, 2023 (Current Framework)
Forensic Scene Investigation	Largely discretionary; investigating officers could choose whether to involve forensic science experts.	Mandatory under Section 176(3) for all offences carrying a punishment of seven years or more imprisonment.
Search and Seizure Protocols	Relied heavily on independent physical witnesses; manual panchnama drafted at the scene.	Mandatory audio-video recording under Section 105; electronic forwarding of recordings to the Magistrate required.
Chain of Custody Documentation	Governed implicitly by judicial precedents, state police manuals, and general administrative guidelines.	Statutorily codified in Section 193(2)(i), strictly requiring chronological custody logs for electronic devices.
Service of Legal Summons	Physical service heavily prioritized; digital service utilized only on an ad-hoc or supplementary basis.	Encrypted electronic summons explicitly authorized and deemed legally valid under Sections 63, 64, and 70.
Modality of Court Proceedings	Relied on periodic Supreme Court guidelines for video conferencing in exceptional circumstances.	Section 530 broadly permits all trials, inquiries, and legal proceedings to be conducted via electronic mode.

The general structure of the procedures in Table 1 is revealing of a clear legislative intent to capture reality at the source by unblinking digital lenses. But, as seen from the lens of AI, the over-reliance on digital devices to ensure integrity of the investigative process creates a significant and largely untouched risk. The procedural protections of the BNSS afford strong protection for a digital crime scene captured by a phone. However, once such a digital file is

slightly manipulated with the help of deepfake technology or generative algorithms and then officially entered into the main system for evidence management, the safeguards of the procedure are unwittingly used to confirm a fake reality (Rimal & Thapa, 2026)¹⁰. The BNSS virtually ignores oversight of the human actors who operate the devices and is entirely silent on the systems needed to identify the possible manipulation of the devices at point of digital capture or immediate post processing. This important procedural "flaw" requires a closer look at the substantive evidence law that complements the BNSS procedural cod.

The Admissibility Threshold and Certification Architecture under the BSA, 2023

The substantive examination of all digital evidence gathered in compliance with the procedures under the BNSS is only governed by the Bharatiya Sakshya Adhiniyam, 2023. The epistemology of electronic evidence is far from the colonial era's traditional, narrow notions of evidence. The epistemology of electronic evidence is distinctly different from the colonial era's narrow, traditional notion of evidence. In what is an explicit recognition of the legal fiction of the past, that digital files were photocopies of some non-existent, physical original machine, electronic and digital records now constitute primary evidence under the specific terms of Section 57 of the BSA (Bidkar, 2026)¹¹. The sweeping change in law recognizes the fact that digital information exists at the same time on many storage media, and each copy is a legal original. The most important and pivotal provision of this new evidentiary regime is Section 63, which supersedes a much more litigated and judicially interpreted Section 65B of the Indian Evidence Act. Section 63 lays out the strict and mandatory standards that must be met for electronic records to be admissible without the production of the original device in court.

The legislature was well aware that digital data is extremely fragile and easily altered, and designed Section 63(4) to act as a strict evidentiary filter. The new dual certification regime found in Section 63(4) significantly increases the technical requirements for the parties who are producing electronic evidence. In compliance with the statutory schedule, a Part A certificate is required, completed by the person responsible for the computer or communication device. Importantly, this Part A certificate shall contain a statement of the hash of the electronic record at issue. A hash value is the result of applying a known cryptographic hash function, like MD5 or SHA-256, to a file, and it acts as a fixed digital fingerprint; if even a single pixel or byte in the file is changed, the hash value will noticeably and drastically change (Sharma & Malviya, 2025)¹³. Plus, the provision requires a Part B certificate (a formal declaration signed

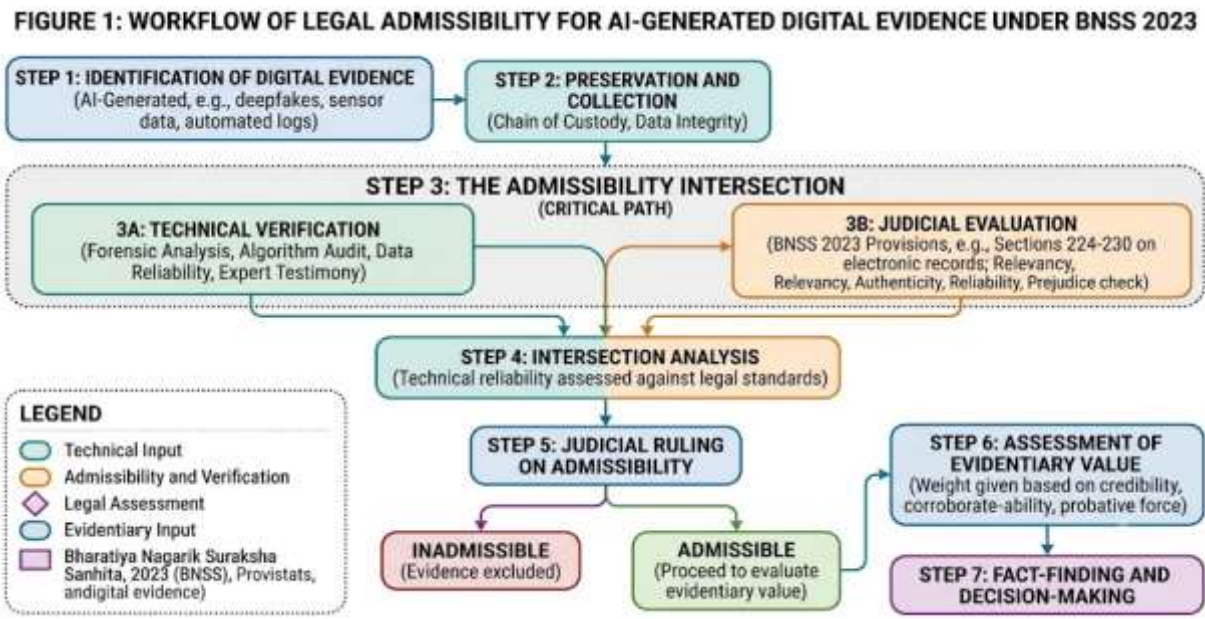
by an expert, offering an additional level of independent technical authentication). The dual-lock mechanism is intended for the Indian courts to ensure there is absolute mathematical proof that an electronic record has not been altered, changed, or knowingly maliciously tampered with, while in transmission, between the seizing officer and the courtroom (JSA Dispute Resolution, 2026)¹⁵.

It is indeed a tough, quite stringent, certification regime, which the Supreme Court of India, in the landmark case of *Pune Bar Association v. Union of India* (2026), upheld as constitutional. In this context, the petitioners in this case strongly contended that it was impossible, burdensome and clearly unreasonable to ask a normal litigant seeking justice to create cryptographic hash values and obtain expert declarations (*Pune Bar Association v. Union of India*, 2026)¹⁶. The Supreme Court, however, rejected this argument altogether, noting in its opinion that electronic records are highly susceptible to continuous change and imperceptible alteration. In an era where AI and deepfake technology have made its way into the world, these inherent vulnerabilities are compounded, the Court said. The Supreme Court therefore determined that the hash value is an integral and non-negotiable electronic fingerprint that affords the assurance of authenticity and integrity, and therefore has a clear and rational connection with the legislative aim of preventing massive miscarriages of justice.

Importantly for the administration of justice in practice, the Supreme Court in the same judgment also set out the precise definition of 'expert' needed for the Part B certificate. The apex court, reversing a very restrictive reading of Section 39(1) given by the Madras High Court, read both clauses in harmony with each other. The Court held that the person who signs Part B does not have to be notified only under Section 79A of the Information Technology Act, 2000. However, it is not only an official expert in computer science and cyber forensics who can legally serve as an expert under the BSA, but any person who has special skills and expertise in computer science and cyber forensics, as demonstrated by a set of evidence, may be qualified as an expert (*Pune Bar Association v. Union of India*, 2026)¹⁷. This judicial interpretation is crucial for litigants because it will help avoid the whole evidentiary framework collapsing due to the lack of officially notified Section 79A examiners (Kapoor, 2026)¹⁸.

The Epistemological Crisis of AI-Generated Evidence and Deepfakes

While the Supreme Court's strong endorsement of the dual-certification process establishes a robust bulwark against the post-creation tampering of digital files, it simultaneously exposes a catastrophic doctrinal inadequacy when the justice system is confronted with AI-generated evidence.



The process of legal admissibility is complex, with technical verification and judicial assessment both playing pivotal roles as illustrated in Figure 1. The underlying premise of the entire conceptual framework of Section 63(4) of the BSA is that the source material is an objective and historical fact that happened, and hence could be identified as such. Even the mathematical wizardry of a hash value only provides assurance that the file appearing in the courtroom is a perfect copy of the file that was produced on the digital device at a certain time. It gives absolutely no mathematical, forensic or logical proof that the event shown in the file actually took place in the physical world.

Let's say a malicious actor is able to use advanced generative adversarial networks (GANs) to generate a highly realistic deepfake video of a politician accepting a bribe or an innocent citizen committing an act of violence and then easily saves that synthetic video to a standard smartphone; then the resulting digital file will have a perfect, immutable hash value (Bajaj & Singh, 2026)19. A hash value given in the Part A certificate required by the BSA will correctly report this value; and a cyber forensic expert completing Part B will accurately and truthfully testify that the file on the phone matches the file presented in court. One might think that the court would formally accept as evidence and admit as testimony the content of the algorithmic hallucination, because it is a formal and mechanical adherence to the procedures of the BSA. This highly chilling phenomenon is an apt description of what scholars have coined the “delusion of objectivity” in the world of digital evidence. The principle of “seeing is believing” is not new in the Indian legal system, as it is in other legal systems around the world. Courts gave tremendous credence to the photographs, audio logs and videotapes because they were thought to be that—the mechanical, objective record of reality, free of human manipulation

and bias. In other words, artificial intelligence completely destroys this paradigm (Rimal & Thapa, 2026)¹⁰. The algorithms for deepfakes are not simply a way to manipulate existing pixels with traditional image editing tools; they create entirely new types of data structures that replicate human micromovements, inflections in speech, natural lighting and more with incredibly high fidelity that is far beyond what can be detected. A recent case of the viral deep fake of a popular Indian actor in 2023 can be used as an example to illustrate that synthetic media can deceive not only the general public but even the untrained forensic experts (Varshita, 2026)⁵.

The typical methods of legal discovery and proof, including cross-examination and presentation of documents, are completely useless from a practical standpoint when the algorithmic evidence is introduced into the judicial process through the BSA. There is no way to cross-examine a generative algorithm, and no way to tell that a synthetic digital artifact is not real with the naked eye. The process of transmission (Varshita, 2026)⁵ is the only one that BSA is concerned with, while creation is a much more dangerous process. It fails to acknowledge that the digital device is an active and intelligent agent, its edge-computing chips and cloud software are active and autonomous, and that they all contribute to the creation of synthetic realities. The implications for criminal jurisprudence are extremely troubling. In the typical scenario of alleged digital forgery, non-consensual synthetic intimate imagery or algorithmic financial fraud, the AI-generated document is not just a piece of evidence of a crime, it is the very crime itself. The outputs of these algorithms can enter the courts as reliable evidence under the ordinary rules of Section 63 of the Evidence Act, without any judicial investigation into the nature of the data used to train the algorithms, error rates of the algorithms, or the algorithmic bias of the underlying software. These algorithmic outputs can enter as reliable evidence in the courts under the ordinary provisions of the Evidence Act 63, without a highly specialized judicial inquiry into the nature of the training data, error rates of the algorithms, or the algorithmic bias of the underlying software. The current legal regime is adequate to ensure that the container is authenticated but it is utterly impotent to respond to the artificiality of the contents, and it could lead to enormously difficult convictions on the basis of mathematical certainties.

Evidentiary Value, Probative Weight, and Algorithmic Transparency

In the age of Artificial Intelligence, the key difference between formal admissibility and substantive evidentiary value turns into the real battleground. If the production of a deepfake using artificial intelligence or a sophisticated computerised process, or the output of a complex

algorithm, is technically admitted to the evidence by a magistrate under Section 63(4) – which is an unprecedented level of formality and precision in the criminal courts – then it will have to be given a level of critical and scientific scrutiny that will determine its probative value in the sense of its weight in proving a fact in issue. Even before the advent of the BSA (Anvar P.V. v. P.K. Basheer, 2014)²⁰, it was realised that in a digitally dominated world, the existence of electronic content alone does not provide much in itself to establish veracity. The Indian courts need to establish their own jurisprudential protections, which go beyond what the BSA explicitly provides for, in order to avoid massively miscarrying justice. This is essentially a change in the standard for admissibility from a certification-based, to a reliability-based, approach to probative evaluation, conceptually similar to the stringent Daubert standard used in the United States, but specifically for extreme opacity of algorithmic evidence (Bajaj & Singh, 2026)¹⁹.

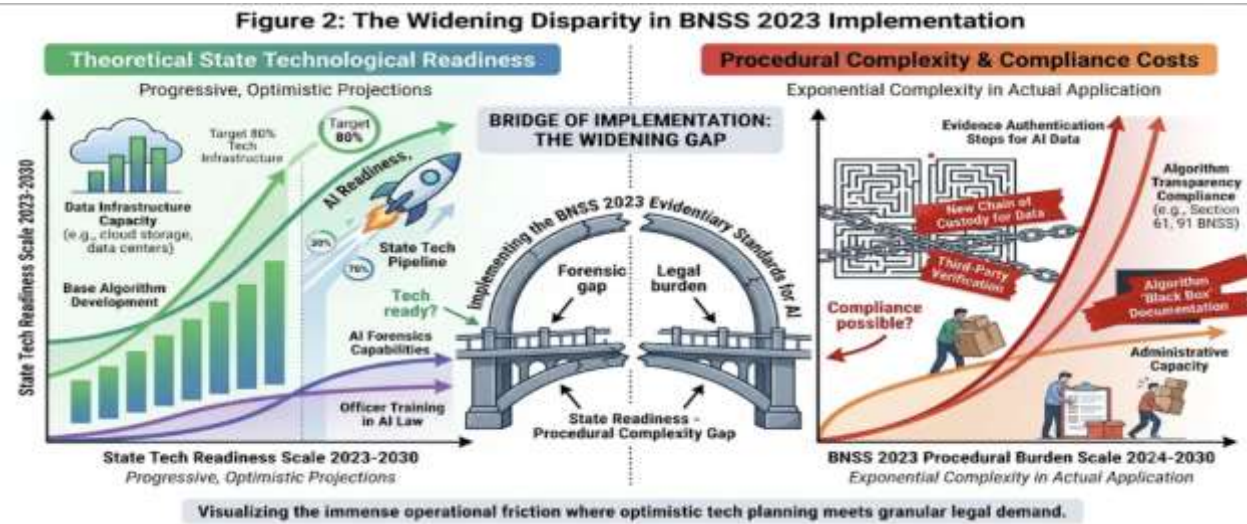
Courts must have the power to require full disclosure of the digital source of the file in assessing the probative value of evidence involving AI. This process is much more than just extracting the metadata. To detect synthetic noise, unnatural pixel blending, temporal inconsistencies and chronometric anomalies that indicate algorithmic generation, forensic investigators need to use sophisticated counter-AI detection software (Sharma & Malviya, 2025)¹³. In addition, where the prosecution relies expressly on the use of an AI system, e.g. facial recognition matches via CCTV footage, predictive policing analytics to establish probable cause, etc., the defence should be afforded unrestricted access to the algorithmic parameters, training datasets and system failure rates for them to challenge the evidence effectively. The opacity of proprietary “black box” AI systems is at odds with the accused's right to a strong defense.

It is a principle that the Supreme Court of India has always respected and valued when it comes to new scientific evidence before the court, that it must be constitutional. In earlier cases, the Court had highlighted that it is unconstitutional to force reliance on untried neurology tests like narco-analysis or brain-mapping – which raise the spectre of torture – on the fundamental right against self-incrimination under Article 20(3) of the Constitution (Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, 2020). The same skepticism towards the constitution that had to be applied to the outputs of the human mind must be applied to AI outputs. The probative value of digital evidence is not what the technology is or how complex it is but what the technology proves and the transparency and demonstrable, legally-interpretable logic behind it. The evidentiary weight of an AI-produced document or one that has been heavily influenced by AI should therefore be presumed to be low unless there is independent (non-digital) organic evidence that substantially corroborates it.

In the case of *Tomaso Bruno v. State of Uttar Pradesh*, 2015²⁰, the isolated digital recording, even if it is perfectly certified under Section 63(4) of the BSA, should not be the sole basis upon which a conviction is recorded for criminal cases. The Indian judiciary should be proactive in laying down an evidentiary burden shifting rule in relation to digital media. If a rule of this sort applies, then the burden of proof would need to pass back to the party introducing the evidence if a plausible, technically sound objection were raised by the defending party that the evidence was a deep fake or otherwise synthetically altered. That party shall then have to demonstrate the evidence's organic human origin beyond reasonable doubt with the use of sophisticated computer forensics. This approach to the probative value of evidence is dynamic and allows for the hard-edged rules of the BSA not to become a convenient and automatic channel for algorithmic perjury and evidence fabrication.

Institutional Capacity and the Forensic Infrastructure Divide

The theoretical beauty and far-reaching nature of BNSS and BSA is seriously undermined by stark infrastructural realities of the modern-day criminal justice system in India. The implicit assumption within the mandatory forensic videography required by the BNSS, as well as with the complex cryptographic certifications required by the BSA, is that there exists a very large law enforcement and forensic ecosystem capable of providing training and tools to implement this requirement. The implicit assumption in the mandatory forensic videography required by the BNSS, as well as on the complex cryptographic certifications required by the BSA, is that a large, technologically sophisticated, and trained law enforcement and forensic ecosystem exists to provide such training and tools. In fact, however, the institutional constraints hampering the adoption of these digital reforms are formidable and can undermine the entire legislative endeavour.



The significant differences between the level of technology that the state was prepared for and the massive amount of procedural intricacy that the new evidentiary laws imposed are well captured in the graph of Figure 2. Although many jurisdictions have the theoretical infrastructure to check basic hash values, the current setup of deepfake detection, synthetic media analysis, and algorithmic traceability is still very fragile (Global Cybersecurity Report, 2025)²⁴.

This critical and empirical examination of the post-implementation reality uncovers a huge and growing gap between urban and rural implementation of the new evidentiary norms. Empirical research done in the last few months since the acts took effect shows that the urban courts have experienced a significant drop in the disposal time of cases and an increase in the convictions for cybercrime cases due to the strong infrastructure and financial support provided under the National e-Courts, Phase III project, whereas the rural courts have been largely incapacitated (Meti, 2025)²⁵. Rural police stations often are not equipped with basic secure devices in which to write down evidence, and reliable internet to send out electronic reports, and rural courts are completely lacking in technical components for efficient verification of Section 63(4) certificates. The sheer lack of cyber forensic personnel in almost all of State Forensic Science Laboratories (SFSLs) creates an instant and huge bottleneck in the process as the signature of a forensic expert is an essential requirement for Part B of the BSA certificate.

Table 2: Institutional and Infrastructural Impediments to Digital Evidence Administration.

Institutional Challenge	Manifestation in the Criminal Justice System	Direct Impact on AI Evidence Evaluation
Forensic Personnel Deficit	Up to 50% vacancies in state forensic laboratories across various jurisdictions.	Massive case backlogs severely delay the Part B certification process required for admissibility.
Deepfake Detection Tooling	Critical lack of state-sponsored, standardized counter-AI forensic software.	Total inability to distinguish organic, reality-based video from synthetically generated media.
Judicial Digital Literacy	Many presiding judges lack specialized, continuous training in computer science and data forensics.	Heavy, uncritical reliance on experts; inability to critically assess algorithmic bias or errors.

Urban-Rural Infrastructure Divide	Heavy concentration of digital infrastructure and funding in metropolitan hubs.	Highly unequal access to digital justice and forensic verification for citizens in rural areas.
-----------------------------------	---	---

The shortage of personnel has significant repercussions on the effectiveness of the criminal laws (Khan & Srivastava, 2026)⁶ and their underlying objectives, as elaborated in detail in Table 2. Whereas according to section 176(3) of the BNSS, police officers are required to hire forensic experts in all serious crimes, but the number of cases is far too huge and the number of forensic experts is limited, this results in an undue delay in charge sheets being filed and the accused's right to a speedy trial is violated. Furthermore, there is no one standard, state-approved software for detecting deepfakes, which means that even if a highly suspect digital file is sent to a regional laboratory the lab examiners might only have tools to verify the hash value, not to test the media for synthetic generation (Rimal & Thapa, 2026)¹⁰.

An empty legislative victory if the state doesn't have the institutional means to interrogate collected evidence. Urgently implementing the National Forensic Infrastructure Enhancement Scheme into the actual operation of the BNSS and BSA is essential for giving life to both Schemes. This demands using AI-powered detection instruments at regional and district level labs and conducting intensive, specialized and ongoing capacity building programme for investigators and judiciary (Shafhi Mohammad v. State of Himachal Pradesh, 2018)³. If these infrastructural investments are not made, the modernization of India's evidence laws will stay in the statute books and do little to shield citizens from the twenty first century's slew of advanced electronic threats.

Conclusion

The Bharatiya Nagarik Suraksha Sanhita, 2023, and Bharatiya Sakshya Adhiniyam, 2023, are clear stepping stones for the Indian legal system to move into the 21st century of digital jurisprudence. The legislature has made forensic investigation a mandatory requirement for crime-solving and given the judiciary and law enforcement agencies the legal tools they need to effectively deal with a technologically complex society, by granting electronic records the same weight as other physical evidence. But as the lawmakers make their triumph, the fast-growing, uncontrolled use of artificial intelligence and deep fake technology also makes its way into the fold. The thorough doctrinal examination of the BSA shows that the structure of the BSA, in particular the use of cryptographic hash values heavily in section 63(4), is designed to prevent tampering after creation only. This makes the entire system useless when it comes

to detecting fabricated evidence at the outset, which is generated by AI. Its form as it stands does indeed "check" the integrity of the digital container, but is dangerously oblivious to the synthetic nature of the contents.

Indian courts need to quickly transcend the limitations of applying a checklist of statutory admissibility to digital evidence and adopt a more dynamic and reliability-oriented framework to evaluate the "true probative value" of digital evidence to ensure constitutional protection of a fair trial and due process. Algorithmic output and digital media should only be considered admissible as evidence if it is subject to rigorous verification and particular expert forensics analyses that can detect synthetic manipulation. When there are credible allegations of deepfake manipulation, the judiciary should be willing to place the burden of proof. Moreover, the successful implementation of these sweeping changes to the criminal law solely depends on addressing the acute gaps in infrastructure that undermine the forensic system today. The progressive recommendations in the BNSS and BSA cannot achieve equitable justice without massive and sustained investments in the development of cyber forensic laboratories, the deliberate raising of judicial digital literacy, both in urban and in rural areas, and the intentional expansion of the use of counter-AI technologies. So long as these gaps persist, the justice system is still at risk of being fooled by algorithms, with innocent convictions and guilty acquittals possible in the digital era.

Works cited

1. Unmasking the Rhetoric of Reform – The Bharatiya Sakshya Adhiniyam 2023 in Context, <https://repository.nls.ac.in/nlsir/vol36/iss1/2/>
2. Digital Criminal Justice: Evaluating the Digital Reforms Introduced under the Bharatiya Nyaya Sanhita and Bharatiya Nagarik Suraksha Sanhita - ResearchGate, https://www.researchgate.net/publication/408495237_Digital_Criminal_Justice_Evaluating_the_Digital_Reforms_Introduced_under_the_Bharatiya_Nyaya_Sanhita_and_Bharatiya_Nagarik_Suraksha_Sanhita
3. ARTIFICIAL INTELLIGENCE, DEEPFAKES, AND THE LAW OF EVIDENCE: AN ANALYSIS UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023 - White Black Legal, <https://www.whiteblacklegal.co.in/index.php/details/artificial-intelligence-deepfakes-and-the-law-of-evidence-an-analysis-under-the-bharatiya-sakshya-adhiniyam-2023-by---dr-arpita-mishra-dr-karunesh-shukla->
4. A COMPARATIVE STUDY OF ELECTRONIC EVIDENCE ADMISSIBILITY: INDIA'S BHARATIYA SAKSHYA ADHINIYAM, 2023 VIS-A-VIS THE US

- FEDERAL RULES OF EVIDENCE AND THE EU eIDAS REGULATION - LIJDLR, <https://lijdlr.com/2026/05/08/a-comparative-study-of-electronic-evidence-admissibility-indias-bharatiya-sakshya-adhiniyam-2023-vis-a-vis-the-us-federal-rules-of-evidence-and-the-eu-eidas-regulation/>
5. Artificial Intelligence-Generated Evidence And Deepfakes Under The Bharatiya Sakshya Adhiniyam, 2023: Rethinking Admissibility And Authentication In Indian Courts, <https://www.ijlrr.com/post/artificial-intelligence-generated-evidence-and-deepfakes-under-the-bharatiya-sakshya-adhiniyam-2023>
 6. The Forensic Investigation Mandate Under the Bharatiya Nagarik Suraksha Sanhita, 2023, and the - IJCRT.org, <https://ijcrt.org/papers/IJCRT2605767.pdf>
 7. BNSS 2023: Electronic Evidence Provisions | PDF | Witness | Arrest - Scribd, <https://www.scribd.com/document/875938921/Bharatiya-Nagarik-Suraksha-Sanhita-EE>
 8. The Bharatiya Nagarik Suraksha Sanhita, 2023 - PRS Legislative Research, <https://prsindia.org/billtrack/the-bharatiya-nagarik-suraksha-sanhita-2023>
 9. The Bharatiya Nagarik Suraksha (Second) Sanhita, 2023 - PRS Legislative Research, <https://prsindia.org/billtrack/the-bharatiya-nagarik-suraksha-second-sanhita-2023>
 10. Digital Evidence In The Era Of Artificial Intelligence: A Doctrinal Study Of Admissibility, Authenticity, And Evidentiary Integrity Under The Bharatiya Sakshya Adhiniyam, 2023, <https://www.ijlrr.com/post/digital-evidence-in-the-era-of-artificial-intelligence-a-doctrinal-study-of-admissibility-authenti>
 11. (PDF) Admissibility of Digital Forensic Evidence Under the Bharatiya, https://www.researchgate.net/publication/407126094_Admissibility_of_Digital_Forensic_Evidence_Under_the_Bharatiya_Sakshya_Adhiniyam_2023
 12. Admissibility of Digital Forensic Evidence Under the Bharatiya Sakshya Adhiniyam, 2023 - IJFMR, <https://www.ijfmr.com/papers/2026/2/74865.pdf>
 13. AN ADMISSIBILITY OF ELECTRONIC EVIDENCE IN CRIMINAL PROCEEDINGS: A COMPREHENSIVE ANALYSIS - Indian Journal of Integrated Research in Law, <https://ijirl.com/wp-content/uploads/2025/11/AN-ADMISSIBILITY-OF-ELECTRONIC-EVIDENCE-IN-CRIMINAL-PROCEEDINGS-A-COMPREHENSIVE-ANALYSIS.pdf>
 14. Re-conceptualizing Section 63 of Bharatiya Sakshya Adhiniyam: Judicial Approach to Electronic Evidence in the Age of AI-Generated Content | Zenodo, <https://zenodo.org/records/15872096>

15. JSA Prism Dispute Resolution, https://www.jsalaw.com/wp-content/uploads/2026/06/JSA-Prism-Dispute-Resolution-June-2026-Electronic-Evidence.Final_.pdf
16. Constitutional validity of Section 63(4) of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) read with its Schedule, which mandates a certificate disclosing hash value of electronic records (Part A) and a declaration by an expert (Part B) as a pre-condition for - GST INDIA Biz, <https://gstindia.biz/case-law/278/pune-bar-association-vs-union-of-india-and-others>
17. Pune Bar Association vs Union Of India on 22 May, 2026 - Indian Kanoon, <https://indiankanoon.org/doc/5836207/>
18. Section 65B & Section 63 BSA Certificate Guide (PDF) - Shonee Kapoor, <https://www.shoneekapoor.com/section-65b-section-63-bsa-certificate-pdf/>
19. ALGORITHMIC EVIDENCE IN THE DOCK: EXAMINING THE ADMISSIBILITY OF AI- GENERATED RECORDS UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 20 - IJLCS, <https://www.ijlcs.in/algorithmic-evidence-in-the-dock-examining-the-admissibility-of-aigenerated-records-under-the-bharatiya-sakshya-adhiniyam-2023-and-the-case-for-a-dedicated-normative-framework>
20. DIGITAL EVIDENCE AND THE CRISIS OF AUTHENTICITY ELECTRONIC PROOF UNDER THE BHARATIYA NAGARIK SURAKSHA SANHITA (BNSS) - JLRJS, <https://jlrjs.com/digital-evidence-and-the-crisis-of-authenticity-electronic-proof-under-the-bnss/>
21. AI-GENERATED EVIDENCE AND ADMISSIBILITY UNDER THE INDIAN EVIDENCE ACT - indian journal of legal review, <https://ijlr.iledu.in/wp-content/uploads/2026/05/V6I881.pdf>
22. New Criminal Laws: Legal Recognition Of Advanced Technology In The Indian Criminal Justice System, <https://www.ijllr.com/post/new-criminal-laws-legal-recognition-of-advanced-technology-in-the-indian-criminal-justice-system>
23. The Bharatiya Sakshya Adhiniyam, 2023 and the Evolution of Evidentiary Standards: Implications for Judicial Remedies, <https://lexscriptamagazine.com/the-bharatiya-sakshya-adhiniyam-2023-and-the-evolution-of-evidentiary-standards-implications-for-judicial-remedies-2/>
24. DEEPFAKES AND THE EVIDENTIARY VOID: CHALLENGES IN AUTHENTICATING AI-GENERATED EVIDENCE UNDER THE BHARTIYA SAKSHYA ADHINIYAM, 202, <https://ijirl.com/wp-content/uploads/2026/04/52.->

[DEEPFAKES-AND-THE-EVIDENTIARY-VOID-CHALLENGES-IN-AUTHENTICATING-AI-GENERATED-EVIDENCE-UNDER-THE-BHARTIYA-SAKSHYA-ADHINIYAM-2023.pdf](#)

25. practical impact and challenges of electronic evidence under the bharatiya sakshya adhiniyam in 2025: a study, <https://ijlr.iledu.in/practical-impact-and-challenges-of-electronic-evidence-under-the-bharatiya-sakshya-adhiniyam-in-2025-a-study/>

