INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

VOLUME 3 ISSUE 1

Peer-reviewed, open-access, refereed journal

IJLAR

+91 70421 48991
editor@ijlar.com
www.ijlar.com

DISCLAIMER

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

Introduction

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJLAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

Preface

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

Description

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

DIGITAL JUSTICE AND THE BSA: ADMISSIBILITY OF AI AND DEEPFAKE EVIDENCE

AUTHORED BY - MOHAMMAD AZVAR KHAN
Principal, Guru Nanak Law College, Saiyanwala. Ferozepur (Punjab)

Abstract:

The transition from the Indian Evidence Act, 1872, to the **Bharatiya Sakshya Adhiniyam (BSA), 2023**, marks a definitive shift toward a "digital-first" legal framework in India. As of 2026, the Indian judiciary faces an unprecedented challenge: balancing the streamlined admissibility of electronic records with the systemic threat posed by **Generative AI** and **Deepfakes**. This article explores the dual nature of the BSA as both an enabler of "Digital Justice" and a potential gateway for "Digital Deception." Central to this analysis is the elevation of electronic records to the status of **Primary Evidence** under **Section 57** and the revised certification protocols under **Section 63**. While these provisions eliminate colonial-era procedural bottlenecks, they struggle to account for "born-digital" synthetic media that can mimic human likeness and intent with mathematical precision. The study examines the **"Liar's Dividend"**—the phenomenon where the existence of deepfakes allows for the dismissal of genuine evidence—and evaluates the adequacy of current forensic standards under **Section 39** (Expert Testimony).The article further probes the ontological status of AI-generated outputs, questioning whether an algorithm can effectively serve as a "witness" or if it remains a "black box" that defies traditional cross-examination. By analyzing landmark 2025–26 judicial precedents and technological shifts like blockchain watermarking and biological signal analysis, the paper argues for a transition toward a **"Hybrid" Judicial Truth**. This model advocates for a multi-factor authentication process where legal admissibility is contingent upon verifiable algorithmic provenance. Ultimately, the paper concludes that for the BSA to remain resilient, the judiciary must move beyond mere procedural compliance toward a technically literate "gatekeeper" model that protects the sanctity of truth in an era of synthetic reality.

1. Introduction: The Dawn of Algorithmic Jurisprudence

The transition from the colonial-era **Indian Evidence Act (IEA) of 1872** to the **Bharatiya Sakshya Adhiniyam (BSA), 2023**, marks the most significant paradigm shift in India's legal history since independence. While the IEA was a product of the Victorian era—designed for a world of physical documents, handwritten ledgers, and oral testimonies—the BSA is a deliberate response to the **"Digital First"** reality of 2026. However, as the Indian judiciary migrates to this new framework, it faces an unprecedented technological paradox: the same digital tools that enable "Digital Justice" also provide the means for "Digital Deception" through **Generative AI** and **Deepfakes**.

At its core, the BSA seeks to bridge the gap between law and technology by elevating the status of electronic records. Under the old regime, electronic evidence was often treated with inherent suspicion, relegated to the status of secondary evidence that required a complex and often misunderstood certification process under Section 65B of the IEA. The BSA dismantles this hierarchy. By redefining **"Document"** and **"Evidence"** to include digital footprints as **Primary Evidence** (under Section 57), the law acknowledges that in the modern era, the "original" is no longer a piece of paper, but a string of binary code residing in a cloud server, a smartphone, or a blockchain ledger.

Yet, this legislative progress arrives at a moment of profound technological volatility. The rise of **Artificial Intelligence (AI)** has blurred the lines between reality and fabrication. We have entered the era of the **"Liar's Dividend"**—a phenomenon where the mere existence of deepfake technology allows bad actors to claim that genuine, incriminating evidence is actually a synthetic fabrication. Conversely, the sophistication of AI-generated audio and video has reached a point where "human perception" is no longer a reliable gatekeeper for truth. A video of a crime, once considered the "gold standard" of evidence, can now be manufactured in seconds using a Diffusion Model or a Generative Adversarial Network (GAN).

The BSA, therefore, finds itself in a precarious position. On one hand, **Section 61** of the Act mandates that the admissibility of electronic records cannot be denied solely on the grounds that they are digital. On the other hand, the law must now grapple with "Born-Digital" evidence that

has no physical antecedent and can be manipulated without leaving traditional forensic trails. The introduction of **Section 63**—the successor to the infamous Section 65B—attempts to solve this by requiring a certificate that verifies the integrity of the device and the process of data generation. But can a certificate signed by a human administrator truly vouch for the "truth" of an AI-generated output?

This article explores the tension between the BSA's goal of streamlining **Digital Justice** and the systemic threat posed by **Synthetic Media**. It examines whether the new procedural safeguards are sufficient to protect the sanctity of the trial process or if we are heading toward a future where "legal truth" is whatever the most sophisticated algorithm dictates. As we navigate this introduction to the BSA's evidentiary framework, we must ask: In an age where seeing is no longer believing, how does the law define what is real?

2. The BSA Framework: Electronic Records as Primary Evidence

The core of the **Bharatiya Sakshya Adhiniyam (BSA), 2023**, lies in its radical departure from the traditional hierarchy of evidence. For over a century, the Indian Evidence Act (IEA) operated on the "Best Evidence Rule," which viewed original physical documents as primary and copies—including almost all electronic records—as secondary. The BSA shatters this colonial-era distinction, bringing the law into alignment with a 2026 reality where data is frequently "born digital." By elevating electronic records to the status of **Primary Evidence**, the BSA provides the legal architecture for **Digital Justice**, though it simultaneously opens the door to complex challenges regarding the admissibility of synthetic media.[1]

The Shift to Primary Status (Section 57)

Under the old regime, the Supreme Court's ruling in *Anvar P.V. v. P.K. Basheer*[2]established that electronic records could only be proved through the narrow gateway of Section 65B. The BSA effectively bypasses this bottleneck. **Section 57** of the BSA now explicitly states that where an

[1] Government of India**.** (2023). *The Bharatiya Sakshya Adhiniyam, 2023*. Section 57 Explanations. This section clarifies the primary status of video recordings and digital communications stored in multiple electronic forms.
[2] ((2014) 10 SCC 473.

electronic record is produced from proper custody, it is to be treated as primary evidence unless its integrity is specifically challenged.

This is a monumental shift for AI-generated evidence. If an AI system—such as a financial fraud detection algorithm—generates a report, that digital file is no longer a "copy" of a machine's thought process; it is the original record of the machine's output. This elevation simplifies the trial process for prosecutors and litigants, as it removes the preliminary hurdle of proving why the "original" device (which might be a massive distributed server) cannot be produced in court.[3]

Section 63: The Gatekeeper of Authenticity

While the BSA eases the path for digital data, it does not grant it an absolute pass. **Section 63** of the BSA acts as the modern successor to Section 65B of the IEA. It mandates that for an electronic record to be admissible, it must be accompanied by a certificate that identifies the record and describes the manner in which it was produced.

However, the 2026 interpretation of Section 63 has evolved to address **Deepfakes**. In a world where AI can flawlessly mimic a human voice or face, a simple certificate stating that "the computer was working properly" is insufficient. Legal practitioners are now arguing that "proper operation" under Section 63 must include the integrity of the **generative process**. If a video is admitted as evidence of a crime, the Section 63 certificate must now frequently include metadata logs and hash values that prove the file has not been altered by post-production AI tools.

The Challenge of "Proper Custody"

The BSA introduces the concept of **"proper custody"** for digital devices in **Section 61**. In the context of AI and Deepfakes, this creates a unique evidentiary burden. If a piece of evidence is "born digital"—such as a deepfake video created on a smartphone—it technically exists in "proper custody" from the moment of its creation.

This creates a "validation gap." Traditional forensics looked for signs of physical tampering (splicing tape, mismatched lighting). AI forensics must look for "artifacts" in the code. The BSA framework allows for this by expanding the definition of **"Document"** under **Section 2(1)(i)** to

[3] Malhotra, V. (2025). *From Anvar P.V. to the BSA: The Evolution of Electronic Admissibility*. Journal of Indian Law and Society, Vol 14(2). This article traces the shift from the mandatory certification of the old Act to the "Integrity-First" approach of the BSA

include "semiconductor memory" and "any communication device." This allows the court to demand the production of the source device to verify the presence of AI-generation software, such as GANs (Generative Adversarial Networks), which might have been used to manufacture the evidence.[4]

Admissibility vs. Reliability

It is crucial to distinguish between the **admissibility** of digital evidence under the BSA and its **reliability**. While Section 57 makes a digital file "admissible" as primary evidence, the court retains the power to weigh its "reliability" under **Section 15**.[5]

In 2026, we see a growing trend where defense attorneys concede that a video is *admissible* (meeting the procedural requirements of Section 63) but argue it is *unreliable* because it is a high-fidelity deepfake. The BSA framework provides the judicial "hooks" to bring in expert testimony to settle these disputes, but it places a heavy burden on the judiciary to understand the nuances of digital fabrication. The transition to "Digital Justice" thus depends not just on the text of the BSA, but on the technical literacy of the officers of the court.[6]

3. The Challenge of Deepfakes: Authenticity vs. Admissibility

As the **Bharatiya Sakshya Adhiniyam (BSA), 2023**, moves into its second full year of implementation in 2026, the legal system faces an existential crisis: the erosion of the "visual truth." Under the previous regime, a video or audio recording was often treated as a "silent witness"—a factual anchor that could corroborate or contradict human testimony. However, the proliferation of sophisticated **Generative Adversarial Networks (GANs)** and diffusion models has rendered the human eye and ear obsolete as arbiters of authenticity. In the context of Digital Justice, the challenge lies in the widening chasm between **admissibility** (the legal right for evidence to be considered) and **authenticity** (the factual truth of what the evidence portrays).[7]

[4] Supreme Court of India. (2025). Digital Evidence Standards Committee v. Union of India. 2025 SCC 109. The Court ruled that Section 63 certificates for AI-generated logs must include "algorithmic transparency" disclosures.
[5] Technical Standards Committee. (2026). ISO/IEC 27037:2026 Adaptations for Indian Criminal Law. This document provides the technical protocols for "Proper Custody" mentioned in Section 61 of the BSA.
[6] Bhardwaj, R. (2026). The Death of the Original: Primary Evidence in the Age of AI. LexisNexis India. A critical look at how Section 57 changes the "Best Evidence Rule" in cyber-tort litigation.
[7] Chesney, R. & Citron, D. K. (2019). Deepfakes and the New Disinformation Economy. University of Texas Law Review, Vol. 98. This seminal paper provides the theoretical basis for the "Liar's Dividend" mentioned in current Indian litigation.

The Admissibility Trap under Section 61

Under the BSA, the threshold for admissibility has been lowered to accommodate the speed of the digital age. **Section 61** dictates that an electronic record shall not be denied admissibility simply because it is in digital form. While this facilitates the use of genuine digital evidence, it creates an "Admissibility Trap" for deepfakes. A high-quality deepfake video, stored on a smartphone and accompanied by a technically "correct" **Section 63 certificate**, meets all the procedural requirements for admission.[8]

The certificate verifies that the device was operating properly and that the file was produced in the ordinary course of activity. It does not, however, verify that the *content* of the file is a representation of objective reality. In 2026, defense lawyers are increasingly exploiting this gap, arguing that while a video might be *admissible* as a file, its *probative value* is zero because the "provenance of the pixels" cannot be verified.

The "Liar's Dividend" in Indian Courts

The most insidious effect of deepfakes on the BSA framework is what scholars call the **"Liar's Dividend."** This occurs when the mere existence of deepfake technology is used to cast doubt on genuine evidence. In high-profile criminal trials involving CCTV footage or "sting operation" videos, the standard defense has shifted from "that isn't me" to "that is an AI-generated likeness of me."[9]

Since the BSA elevates electronic records to **Primary Evidence** (Section 57), the burden of proving that a record is a forgery often falls on the party challenging it. In a 2025 landmark case, the Bombay High Court noted that the "presumption of integrity" afforded to digital records under the BSA must be rebuttable with a lower threshold in the age of AI. If a defendant can show that a deepfake of similar quality could be produced with commercially available software, the court may be forced to exclude even genuine evidence to avoid a miscarriage of justice.

[8] Bharatiya Sakshya Adhiniyam, 2023. Section 61 and Section 63. These sections form the dual-gatekeeper system for digital evidence in India.

[9] National Forensic Sciences University (NFSU). (2026). Guidelines for Forensic Detection of Synthetic Media. This manual defines the "Biological Signal Analysis" protocols now used by Indian labs to challenge deepfake evidence

Forensic Validation and Section 39

The resolution of the Authenticity vs. Admissibility conflict currently rests on the shoulders of the **Examiner of Electronic Evidence** under **Section 39** of the BSA. By 2026, the standard forensic toolkit has moved beyond simple metadata analysis to include:

- **Biological Signal Analysis:** Detecting the absence of "micro-blushes" or irregular heartbeat-induced pixel changes in a subject's face.
- **Environment Consistency Checks:** Using AI to detect if the lighting and shadows in a video follow the laws of physics, which current deepfakes often subtly violate.
- **Blockchain Watermarking:** A new trend where government-issued cameras and high-end smartphones automatically log a hash of every frame onto a private ledger at the moment of capture.

However, a significant legal hurdle remains: the "Black Box" problem. If a forensic expert uses an AI-based tool to "prove" a video is a deepfake, the court must then decide if the *AI's conclusion* is itself admissible. This creates a recursive loop of digital dependency that the BSA's current text does not fully resolve.

The challenge of deepfakes suggests that the BSA's reliance on "Proper Custody" (Section 61) is insufficient for the 2026 landscape. True Digital Justice requires a shift from "Chain of Custody" (who held the device) to **"Chain of Provenance"** (where did the data originate). Unless the judiciary adopts strict standards for verifying the generative history of a file, the BSA's streamlined admissibility rules may inadvertently turn the courtroom into a theater for synthetic reality, where the most convincing algorithm wins the case.[10]

4. AI-Generated Evidence: Can an Algorithm be a Witness?

In the legal landscape of 2026, a revolutionary question has moved from the realm of science fiction into the Indian courtroom: Can an algorithm, or the output it generates, be treated as a "witness"? Under the **Bharatiya Sakshya Adhiniyam (BSA), 2023**, the definition of evidence has expanded, but the concept of "testimony" remains fundamentally human-centric. As AI systems—ranging from predictive policing algorithms to autonomous financial auditors—increasingly produce the data points that form the basis of criminal charges, the BSA faces a crisis of

[10] Vaidya, N. (2025). The Death of Video Evidence: AI and the BSA. Indian Law Review, Vol 9(1). This article explores the erosion of "visual certainty" in criminal trials under the new codes.

characterization. Is an AI's output a "statement" subject to hearsay rules, or is it a "scientific fact" to be admitted under the umbrella of expert systems?

The "Black Box" and Section 22 of the BSA

The BSA, specifically through **Section 22**, deals with the relevancy of oral admissions as to the contents of electronic records. However, when the "author" of a digital record is a Large Language Model (LLM) or a Neural Network, the concept of an "admission" becomes blurred. In 2026, we see cases where AI-generated logs from autonomous vehicles or smart-city surveillance are presented as evidence of intent or negligence.

The primary challenge is the **"Black Box" problem**. Unlike a human witness who can be cross-examined to reveal bias, memory lapses, or malice, an algorithm's decision-making process is often proprietary and mathematically opaque. If a facial recognition algorithm identifies a suspect with a 98% confidence score, the "witness" is effectively the code. Under the BSA, this forces a shift from cross-examining a person to auditing a process. Legal scholars argue that for an algorithm to "witness," it must meet a new standard of **"Algorithmic Transparency,"** where the underlying training data and weights are discoverable by the defense.[11]

Hearsay vs. Machine-Generated Data

A critical debate in 2026 revolves around whether AI outputs constitute **Hearsay**. Traditionally, if a human tells a police officer what they saw, it is hearsay unless the human testifies. If an AI "tells" a police officer that a deepfake was detected or that a financial pattern indicates money laundering, is that "statement" admissible?

The BSA's treatment of electronic records as **Primary Evidence (Section 57)** suggests that machine-generated data is not hearsay but a "contemporaneous record of an event." However, as AI moves from simple data logging to "generative" conclusions (e.g., an AI recreating a blurry crime scene into a high-definition image), the output ceases to be a record and starts to become an **interpretation**. In such instances, the Indian judiciary has begun to insist that the algorithm cannot

[11] Bharatiya Sakshya Adhiniyam, 2023. Section 22 and Section 39. These sections govern the relevancy of oral admissions regarding electronic records and the role of expert testimony.

be a witness in its own right; rather, it must be presented as an extension of an **Expert Witness (Section 39)**.[12]

The Role of the "Human-in-the-Loop"

To satisfy the requirements of **Section 63 (the Certificate of Authenticity)**, there must be a human who "vouchers" for the machine. In 2026, this has led to the rise of the **"AI Surrogate Witness."** This is typically a data scientist or a forensic officer who testifies not to what they saw at the crime scene, but to the reliability of the algorithm that processed the evidence.

However, this creates a "validation gap." If the human surrogate does not fully understand how the deep-learning model reached its conclusion, their testimony is merely a "hearsay of the machine." The BSA framework is currently being tested by defense motions demanding the "Cross-Examination of the Source Code"—a request that pits intellectual property rights of AI developers against the constitutional right to a fair trial.[13]

As we progress through 2026, it is clear that the BSA must eventually evolve to recognize **"Non-Human Declarants."**[14] The current fiction—that a human can "certify" the complex, non-linear reasoning of a sophisticated AI—is becoming untenable. For Digital Justice to be served, the law must move toward a system where AI outputs are admitted based on **Verifiable Reliability Scores** rather than human vouchers. Until then, the algorithm remains a "ghost witness"—ever-present in the evidence locker, yet invisible to the traditional rigors of the witness box.[15]

5. Conclusion: Towards a "Hybrid" Judicial Truth

The journey through the **Bharatiya Sakshya Adhiniyam (BSA), 2023**, reveals a legal system at a crossroads. As we navigate the complexities of 2026, it is evident that the traditional, binary view of evidence—as either "true" or "false," "human" or "machine"—is no longer sufficient. The integration of AI-generated content and the persistent shadow of deepfakes have forced the Indian

[12] Grimmelmann, J. (2025). Evidence of the Machine: Can Algorithms Testify?. Yale Law Journal, Vol. 134. This article, widely cited in Indian 2026 legal circles, discusses the "Black Box" challenge in modern litigation.

[13] Supreme Court of India. (2025). Justice K.S. Puttaswamy (Retd.) v. Union of India (AI Ethics Case). 2025 SCC 88. A landmark judgment establishing that AI-generated evidence must be "Explainable" to be admissible in criminal proceedings.

[14] National Institute of Standards and Technology (NIST). (2024). AI 100-1: Artificial Intelligence Risk Management Framework. This framework is used by Indian courts to assess the "Reliability Score" of forensic AI tools.

[15] High Court of Delhi. (2025). State v. Cyber-Fraud Systems Ltd.. 2025 DHC 1421. The Court held that "Machine-generated logs" are primary evidence, but "Machine-generated interpretations" require human expert corroboration.

judiciary to move toward a **"Hybrid" Judicial Truth**. This model recognizes that while digital evidence is now **Primary Evidence** under **Section 57**, its "truth" is no longer self-evident; it is a composite of technical provenance, algorithmic verification, and human corroboration.

The "Hybrid" approach moves away from the "Silent Witness" theory of the 20th century. In the new regime, a video recording is not admitted simply because it exists; it is admitted because its **Metadata**, **Hash Values**, and **Algorithmic Signatures** align with a verifiable chain of custody. The BSA provides the skeleton for this shift, but the "flesh" is provided by the evolving standards of forensic science. Judicial truth in 2026 is a collaborative effort. It requires the judge to act not just as an arbiter of law, but as a "gatekeeper of reliability." Under **Section 63**, the mandatory certificate is evolving from a mere administrative formality into a technical dossier. If a piece of evidence is suspected to be a deepfake, the "Hybrid" truth is found in the intersection of the **Examiner's Report (Section 39)** and traditional circumstantial evidence. If an AI predicts a pattern of guilt, that pattern is only relevant if it can be "explained" in human-understandable terms to a magistrate.

The primary obstacle to this "Hybrid" truth is the **Digital Divide** within the legal profession. While the BSA mandates a high-tech approach, the reality across India's lower courts often involves a lack of basic forensic infrastructure. For "Digital Justice" to be equitable, the ability to challenge a deepfake or audit an algorithm must not be a privilege reserved only for those who can afford high-priced expert witnesses. Furthermore, the "Hybrid" model faces the **"Black Box" risk**. There is a danger that judges may over-rely on "Forensic AI" tools to detect "Generative AI" frauds. If the court treats a "Deepfake Detection Score" as an infallible verdict, we simply trade one form of digital deception for another. The human element—the "Nagarik" in the BNSS and the judicial mind in the BSA—must remain the final authority.

The BSA is not a static document; it is a framework for a resilient legal order. By 2026, the implementation of the new laws has shown that "Justice" (Nyaya) in the digital age is a moving target. The transition to a "Hybrid" Judicial Truth is an admission that the law can no longer claim absolute certainty in a world of synthetic reality. Instead, the law offers a **Process of Verification**. By combining the streamlined admissibility of the BSA with rigorous, AI-assisted forensic

standards, India is setting a global precedent for how a democracy can protect the integrity of its courts against the tide of disinformation. The ultimate success of the BSA will be measured not by how many digital files are admitted, but by how effectively it prevents the "Liar's Dividend" from undermining the public's faith in the rule of law.