
INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

**DEEPPAKES AND THE VISUAL CHAIN OF CUSTODY: EVALUATING
EVIDENTIARY INTEGRITY UNDER THE BHARATIYA SAKSHYA
ADHINIYAM, 2023**- Tejasvi¹**ABSTRACT**

Deepfakes, the hyper-realistic, AI Generated synthetic media has precipitated an existential crisis for the administration of criminal justice globally and within India. For over a century, the Indian legal system operated on the visual epistemic assumption that "seeing is believing," treating video recordings, CCTV footage, and photographs as highly cogent, objective pieces of documentary proof. However, AI can now synthesise human likenesses and voices with near perfect fidelity, rendering this assumption obsolete. This paper analyses the vulnerabilities of digital evidence under the new criminal law architecture of India, specifically focusing on the Bharatiya Sakshya Adhiniyam, 2023. Examining the intersection of Section 63 of the BSA, the Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita, 2023 (BNS), the paper identifies critical gaps in the new dual-certification regime (Part A and Part B of the Schedule). It further evaluates the constitutional vulnerabilities under Articles 19, 20(3), and 21 of the Constitution of India, particularly highlighting the emergence of the "liar's dividend." Finally, it offers concrete, systemic recommendations for law enforcement, forensic laboratories, and the judiciary to re-engineer a robust "visual chain of custody" utilising cryptographic watermarking, mandatory blockchain-based hashing at the point of ingestion, and specialised judicial training.

THE EXORDIUM

The foundational architecture of the Indian law of evidence was drafted in the late nineteenth century, an era dominated by tangible, physical items. As technology advanced, the judiciary incrementally expanded its interpretation of documents to accommodate tape recordings, magnetic

¹ Advocate at Rajasthan High Court

disks, and eventually digital outputs. Throughout this evolution, a stable jurisprudential thread persisted: while oral testimony could be tainted by human malice, bias, or memory decay, a machine generated record was presumed to capture an immutable slice of reality.

The advent of Deepfakes, synthetic audio, video, or images generated through artificial intelligence that convincingly depict individuals saying or doing things they never did, has fundamentally shattered this paradigm. Built on Generative Adversarial Networks (GANs), where two neural networks (a generator and a discriminator) compete to create and refine flawless fabrications, Deepfakes have shifted digital manipulation from crude pixel editing to sophisticated semantic deception. This technological shift introduces an unprecedented procedural crisis. The threat is two fold:

The Ingestion of Fabricated Proof: Innocent individuals can be falsely implicated in severe criminal offenses, ranging from financial fraud under the Bharatiya Nyaya Sanhita, 2023 (BNS) to offenses against the state, via synthetic digital video files that look indistinguishable from real recordings.

The "Liar's Dividend": Conversely, a guilty defendant can weaponise the known existence of Deepfake technology to introduce reasonable doubt, asserting that a perfectly authentic, incriminating video recording is merely an AI Generated fake.

This erosion of truth undermines the "visual chain of custody", the unbroken chronological record documenting the collection, custody, transfer, and analysis of digital video or audio material. As India transitions into its newly overhauled criminal code framework, evaluating whether our evidentiary statutes can withstand this epistemic shock is not an academic exercise; it is an urgent structural necessity.

The Statutory Framework: Section 63 of the BSA and the Dual Certification

Regime

With the enforcement of the Bharatiya Sakshya Adhiniyam, 2023 (BSA), the legal matrix governing electronic records underwent its most significant transformation since the year 2000. Under the erstwhile regime, Section 65B of the Indian Evidence Act, 1872 dictated the admissibility of electronic records. That framework was heavily litigated, culminating in the landmark Supreme Court decision in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, which held that an electronic certificate was an absolute condition precedent for admitting secondary electronic evidence.

The BSA attempts to streamline and fortify this process. Section 63 of the BSA retains the core four

fold substantive conditions of the old Section 65B:

The regular use of the computing device,

The ordinary feeding of data during normal activities,

The proper functioning of the system during the material period, and The faithful reproduction of the original record.

However, Section 63(4) of the BSA introduces a critical structural shift by mandating a standard-form certificate set out in the Schedule to the BSA. This certificate is divided into a strict dual-certification model:

Part A: To be filled and signed by the person in charge of the computer, communication device, or management of the relevant activities, affirming the lawful possession and proper operation of the source system.

Part B: To be filled and signed by a qualified expert, explicitly demanding the disclosure of the hash value of the electronic or digital record.

The Doctrinal Gaps in Section 63 of the BSA

The fundamental flaw is that Section 63 treats admissibility primarily as a question of system and transmission integrity, rather than content authenticity. If a bad actor creates a high-quality Deepfake video on an external AI platform, transfers it onto a pendrive, and drops that file onto a target smartphone, the smartphone's owner can fill out Part A in complete honesty: the phone was working fine, data was fed in the ordinary course, and the output is a faithful print of what is stored on the memory.

Similarly, a forensic technician completing Part B can run a standard SHA-256 or MD5 cryptographic algorithm and certify a precise hash value. The hash value will perfectly match the file as it existed on that smartphone. Yet, the entire substance of the video is an algorithmic fabrication.

Section 63 operates on the assumption that if the container (the device and the file path) is secure, the contents must be real. Deepfakes break this logic by populating secure, perfectly legal containers with completely engineered data.

Furthermore, the statutory language of Section 63(4)(c) mandates that the certificate must accompany the electronic record "at each instance where it is being submitted for admission." This creates an immense procedural hurdle in multi-tiered trials. If the original hash value is recorded

months after the initial incident or after the file has undergone automated compression over messaging networks like WhatsApp, the hash value changes completely, even if no malicious alteration occurred. The law fails to distinguish between safe metadata compression and malicious content manipulation.

The Collapse of the Traditional "Chain of Custody"

In standard criminal jurisprudence, the chain of custody is a foundational requirement to prevent tampering, substitution, or contamination of evidence. For physical items like a weapon, police track the recovery, bagging, sealing, and safe transit to the Forensic Science Laboratory (FSL). For digital video data, the chain of custody has historically relied on tracking the physical media storage (CCTV hard drives, memory chips) and verifying metadata.

Deepfakes render this conventional pipeline obsolete. A visual chain of custody must verify not just where the file went, but what happened inside the pixels from the exact millisecond the sensor captured the light.

When law enforcement officers seize digital video evidence, they typically rely on basic EXIF (Exchangeable Image File Format) data and file meta data to establish time stamps, GPS coordinates, and device manufacturing models.

Advanced generative tools can alter or generate fake metadata with minimal effort. An automated AI script can output a Deepfake video while injecting synthetic metadata that perfectly mirrors the target's phone camera model, focal length, and local geographical coordinates. When the police extract this file using standard forensic tools like Oxygen Forensics, the extraction report will show a file that appears entirely organic to the device.

Currently, Indian FSLs rely on traditional Deepfake detection methods, which look for visible artifacts such as:

1. Inconsistent blinking patterns or irregular eye tracking,
2. Asymmetric shadows or lighting misalignments across facial planes,
3. Boundary blurring around the neck, ears, and jawline, and
4. Spectral anomalies in audio frequencies.

However, the field of generative AI operates as an asymmetric arms race. The moment a detection algorithm identifies a specific artifact (e.g., lack of realistic eye blinking), developers integrate that parameter directly into the generator network's loss function. The AI learns from its mistake and outputs a newer iteration of the Deepfake that blinks perfectly.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

Consequently, by the time a criminal trial moves from the filing of the chargesheet under Section 193 of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) to the actual stage of cross-examination, the forensic tools used during the initial investigation may be completely obsolete against the generation of Deepfakes used in the crime.

Constitutional Implications

The crisis of the visual chain of custody directly collides with fundamental constitutional guarantees under Part III of the Constitution of India.

Article 21: The Right to a Fair Trial and Due Process

The right to a fair trial is an integral component of the Right to Life and Personal Liberty under Article 21. If the state relies on digital video evidence where the visual chain of custody cannot be robustly verified, the presumption of innocence is fundamentally compromised.

In *Selvi v. State of Karnataka*, the Supreme Court recognised that the forced infusion of unscientific or unreliable forensic techniques into the judicial process violates due process. Admitting a video file that is susceptible to deep-learning manipulation without a verified, granular record of its cryptographic provenance amounts to a trial by ambush, stripping the accused of a meaningful opportunity to defend themselves.

Article 20(3): The Right Against Self-Incrimination

A more complex constitutional dilemma arises when a court attempts to resolve a Deepfake claim. If an accused asserts that a video is a Deepfake, can the court compel them to provide biometric data, facial scans, or voice samples to run a comparative AI forensic analysis?

Under the *State of Bombay v. Kathi Kalu Oghad* paradigm, compelling an accused to give physical prints, handwriting samples, or voice prints for identification does not violate Article 20(3) because it does not constitute "testimony." However, generating a high-fidelity dynamic 3D facial mesh or an extensive vocal recording to train a Deepfake discriminate or network goes far beyond basic static identification. It requires active behavioural output, which could cross the line into compelled self-incrimination, especially if the AI models derive cognitive behavioural traits from the sample.

Systemic Recommendations

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

I. Cryptographic Provenance and Controlled Capture Frameworks

Instead of relying on easily altered post-facto metadata, Indian law enforcement must adopt secure capture frameworks built on open standards like the Coalition for Content Provenance and Authenticity (C2PA).

When a police officer records a video at a crime scene or extracts CCTV footage under the BNSS, the recording application should cryptographically bind the device sensor data, timestamp, and location coordinates directly into the file using a hardware-protected cryptographic key. Any subsequent attempt to re-encode, compress, or alter pixels would automatically break this cryptographic seal, instantly alerting the defense and the court to a breach in the visual chain of custody.

II. Implementation of Decentralised Police Ledgers

The state should establish an immutable, blockchain-based decentralised ledger system for digital evidence ingestion. The moment an electronic record is seized by an investigating officer, its SHA-256 hash value must be uploaded immediately to a secure, time-stamped public-private ledger before it is transferred to FSL or police servers.

When the evidence is presented before the judge, Part B of the Section 63 BSA certificate can simply cross-reference the file's current hash against the ledger's original time stamp entry. If there is a single bit of difference, the evidence should be deemed automatically inadmissible.

III. Statutory Amendments to the BSA Schedule

The legislature must amend the Schedule to the BSA to explicitly address synthetic media. The certificate should require the expert signing Part B to specify: The exact digital forensic tools used to test for GAN or diffusion-model signatures, The error margins and false-positive rates of the detection software deployed, and a clear log verifying that the file's resolution, framerate, and compression history match its reported origin device.

IV. Specialised Judicial and Bar Training

Judges cannot remain passive observers in this technological shift. The National Judicial Academy, Bhopal and State Judicial Academies must introduce intensive technical modules focused on synthetic media, machine learning, and digital forensics. District Court Judges must learn to evaluate digital records critically, ensuring that the presence of a signed certificate does not blind the court to underlying content manipulation.

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

Conclusion

Deepfakes represent a permanent shift in how our courts must interact with digital reality. The long standing legal shortcut that treated video evidence as an absolute mirror of truth is gone.

As Indian advocates navigating the newly enacted Bharatiya Sakshya Adhiniyam, 2023, our duty to our clients and to the court requires a highly rigorous approach to electronic authentication. Section 63 of the BSA provides a helpful foundational structure with its dual-certification model, but it remains dangerously focused on system containers rather than content data.

By implementing cryptographic provenance tracking, securing the ingestion pipeline via decentralised ledgers, and modernising forensic standards, the Indian legal system can bridge this technological gap. We must ensure that our laws evolve fast enough to preserve the integrity of our courts, protect individual liberties, and rebuild a trustworthy visual chain of custody fit for the digital era.

References

- Bharatiya Sakshya Adhiniyam, 2023, §63, No. 47 of 2023 (India).
- Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).
- Ian Goodfellow et al., Generative Adversarial Nets, 27 Advances in Neural Information Processing Systems 2672 (2014).
- Bobby Chesney & Danielle Citron, Deepfakes and the New Disinformation Disruptions, 116 Mich. L. Rev. 1753 (2018).
- Information Technology Act, 2000, §65, §66C, §66D, No. 21 of 2000 (India).
- Bharatiya Nyaya Sanhita, 2023, § 316, § 318, § 336, No. 45 of 2023 (India).
- Anvar P. V. v. P. K. Basheer, (2014) 10 SCC 473 (India).
- Bharatiya Nagarik Suraksha Sanhita, 2023, §193, No. 46 of 2023 (India).
- Coalition for Content Provenance and Authenticity (C2PA), Specification Version 1.3, C2PA Organic Docs (2023).
- Selvi v. State of Karnataka, (2010) 7 SCC 263 (India).
- India Const. art. 21.
- State of Bombay v. Kathi Kalu Oghad, 1962 AIR 1808 (India).
- India Const. art. 20, cl. 3.
- Justice K. S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1 (India).

For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

- Farhana Begum Choudhury, Hash Value For Electronic Evidences, LiveLaw (May 24, 2026), <https://www.livelaw.in/articles/hash-value-electronic-evidences-535457>.
- Saji Koduvath, Sakshya Adhiniyam Mandates Hashing the Original; Established Jurisprudence Requires Hashing the Copy Also, Indian Law Live (June 29, 2025), <https://indianlawlive.net/2025/06/29/sakshya-adhiniyam-doesnt-mandate-hashing-copy-pen-drive-or-cd-produced-it-mandates-hashing-original-only/>.
- Dr. Jineesh Soni, Section 63B SA 2023: Defence Against Electronic Evidence, YouTube (May 13, 2026), <https://www.youtube.com/watch?v=LdnYcGQTRqA>.



For general queries or to submit your research for publication, kindly email us at ijalr.editorial@gmail.com

<https://www.ijalr.in/>

© 2026 International Journal of Advanced Legal Research