2026 Volume: 02 Issue: 11 www.ijrpa.com ISSN 2456-9995 Research Article

International Journal Research Publication Analysis

Page: 01-09

# AI-GENERATED EVIDENCE AND THE FUTURE OF CRIMINAL TRIALS IN INDIA

***Bhargav Anil Patel**

A Legal Research Article on Synthetic Media, Electronic Evidence and Criminal Adjudication in India.

**Article Received: 22 September 2026**
**Article Revised: 12 October 2026**
**Published on: 01 November 2026**

***Corresponding Author: Bhargav Anil Patel**

A Legal Research Article on Synthetic Media, Electronic Evidence and Criminal Adjudication in India.

DOI: https://doi-doi.org/101555/ijrpa.5205

## ABSTRACT

Artificial intelligence is changing the nature of digital evidence. Images, videos, voices, documents and other forms of synthetic media can now be generated or altered with a degree of realism that makes traditional visual inspection increasingly unreliable. For Indian criminal justice, this development is significant because the evidentiary framework has already moved decisively toward electronic and digital records through the Bharatiya Sakshya Adhiniyam, 2023 (BSA), while the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS) strengthens technology-assisted investigation and trial procedures. The central legal problem is no longer simply whether a digital record can be produced before a court, but whether its origin, integrity, authenticity and reliability can be demonstrated when artificial intelligence may have created or modified it. This article examines the existing Indian framework, the evidentiary difficulties created by deepfakes and other AI-generated material, the relevance of chain of custody and expert examination, and the constitutional implications for fair trial rights. It argues that Indian courts should adopt a technology-neutral but authenticity-sensitive approach: AI-generated material should not be automatically excluded, but neither should apparent realism be treated as proof of truth. The article proposes procedural safeguards including provenance documentation, forensic verification, disclosure of relevant metadata, expert standards, judicial training, and clear rules for challenging synthetic evidence. The future of criminal trials will therefore depend not on resisting artificial intelligence, but on developing reliable methods for distinguishing trustworthy digital evidence from persuasive digital fabrication.

**KEYWORDS:** Artificial Intelligence; Deepfakes; Digital Evidence; Bharatiya Sakshya Adhiniyam, 2023; Criminal Trials; Electronic Records; Chain of Custody; Fair Trial.

## 1. INTRODUCTION

Criminal trials are built around a basic judicial task: determining facts from evidence while protecting the accused against wrongful conviction. For decades, courts have evaluated eyewitnesses, documents, photographs, recordings and physical objects. The rapid development of artificial intelligence is altering this landscape. A photograph can now be generated without a camera, a voice can be synthetically reproduced from a short sample, and a video can be manipulated so convincingly that an ordinary viewer may struggle to identify the alteration. The resulting challenge is particularly serious in criminal proceedings because evidence may influence arrest, bail, framing of charges, conviction and sentencing.

India is entering this technological period at the same time as it has substantially reorganised its criminal-law framework. The Bharatiya Sakshya Adhiniyam, 2023 expressly recognises electronic or digital records and contains dedicated provisions dealing with their proof and admissibility. The Bharatiya Nagarik Suraksha Sanhita, 2023 also recognises audio-video electronic processes and permits trials and proceedings to be conducted through electronic modes. These changes provide a legal foundation for modern digital evidence, but they were not designed exclusively for generative artificial intelligence.

The central question, therefore, is not whether AI-generated evidence is 'digital'. It plainly is. The more difficult question is whether a court can establish what created the material, whether it was altered, who controlled the relevant device or account, whether the evidence has remained intact, and whether the proposition for which it is tendered is actually supported by reliable information. An AI-generated image may be genuine evidence of the fact that somebody generated that image, while being completely unreliable as evidence that the depicted event occurred.

This distinction between authenticity and truth should become a central principle of future criminal adjudication. Courts must evaluate the evidentiary foundation behind synthetic media rather than relying on appearance, technical complexity or confidence of the person producing it.

## 2. The Indian Legal Framework for Digital Evidence

The BSA marks an important transition from the older Indian Evidence Act, 1872. Section 61 recognises electronic or digital records, while Sections 62 and 63 establish special provisions

concerning electronic records and their admissibility. The statutory scheme reflects the reality that modern transactions and investigations generate evidence in digital form. Messages, recordings, computer outputs, cloud-stored material, surveillance footage and other electronic information can therefore enter criminal proceedings subject to the statutory requirements.

The earlier judicial development remains highly relevant to understanding the new regime. In Anvar P.V.V.P.K. Basheer, the Supreme Court treated the statutory requirements governing electronic records as a special evidentiary framework. In Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, the Court further clarified the importance of certification requirements under Section 65B of the former Evidence Act and discussed the circumstances in which the law operates in relation to electronic records. The BSA now contains its own provisions, so lawyers must apply the current statutory language rather than mechanically importing every detail of the former Section 65B framework.

The BNSS complements the evidence framework. Section 105 specifically addresses recording of search and seizure through audio-video electronic means, while Section 530 permits trials and proceedings to be held in electronic mode. Such provisions indicate a broader legislative movement toward technologically supported criminal procedure. The Information Technology Act, 2000 also provides a statutory basis for notified examiners of electronic evidence under Section 79A, allowing expert opinion regarding electronic-form evidence.

Yet admissibility is not synonymous with reliability. A file can satisfy formal requirements and still be challenged on the ground that it has been manipulated, incompletely presented, taken out of context or generated through a deceptive process. The judicial inquiry must therefore proceed in stages: identification of the digital object, proof of its provenance, assessment of integrity, evaluation of the method by which it was created or recovered, and finally consideration of its relevance and probative value.

### 3. What Makes AI-Generated Evidence Different?

Traditional digital evidence generally records an event that has already occurred: a CCTV system captures an image, a telephone records a call, or a device stores a message. AI-generated evidence introduces a new category in which software can manufacture content that resembles a record of an event without the event necessarily having occurred.

This is most visible in deepfakes. A face may be superimposed onto another person's body; speech can be cloned; facial expressions can be synthesised; photographs can be generated from text prompts; and existing footage can be altered. The danger is not confined to

sophisticated criminal conspiracies. Consumer-level tools increasingly make synthetic media accessible to ordinary users.

The legal significance lies in the difference between a recording and a representation. A conventional CCTV clip ordinarily purports to preserve sensor-generated information from a particular time and place. An AI-generated video may instead represent an imagined event. If the prosecution presents it as a recording without disclosing its synthetic origin, the evidentiary problem becomes fundamental.

AI also creates an attribution problem. Even if a file is genuine, the court may need to determine who created it, who possessed the device, whether an account was compromised, and whether the content was uploaded by the accused or by another person. Metadata can assist, but metadata itself may be modified. Hash values can demonstrate that a particular digital copy has remained unchanged after acquisition, but a hash cannot prove that the original content was truthful.

Accordingly, future courts should avoid a simplistic 'real or fake' binary. Digital evidence may occupy several categories: authentic recording; authentic recording that has been edited; synthetic content honestly disclosed as synthetic; synthetic content falsely presented as an authentic recording; or evidence whose provenance cannot be established. Each category should receive a different evidentiary assessment.

## 4. The Problem of Deepfakes in Criminal Trials

The most serious risk posed by deepfakes is wrongful attribution. Suppose a video apparently shows an accused committing violence. If the video is accepted as authentic, it may appear to provide direct and powerful proof. If it is synthetic, the same video could become an instrument of deliberate fabrication. The danger is magnified because human observers tend to give visual and auditory information substantial persuasive weight.

The defence may face difficulties that are not present with ordinary documentary evidence. A person may know that a video is false but lack the technical resources to prove how it was created. Expert examination can be expensive and time-consuming. The original device may be unavailable. Online platforms may retain limited information about the creation or upload process. Compression, re-encoding and ordinary editing can also complicate forensic analysis.

There is also a risk of the 'liar's dividend': once synthetic media becomes common, genuine recordings may themselves be dismissed as fake. This can damage both prosecution and defence cases. A legal system that responds to deepfakes only by distrusting digital

evidence would therefore create a second problem—making reliable evidence easier to deny.

The appropriate response is disciplined verification. Courts should ask what the evidence purports to establish, what its source is, how it was obtained, whether the original is available, whether there are independent corroborating records, whether the file has been altered, and whether qualified examination supports the claimed provenance. Where uncertainty remains, the weight of the evidence should be assessed in the context of the entire case rather than treating the disputed file as conclusive.

## 5. Chain of Custody and Digital Provenance

Chain of custody is especially important where evidence is capable of being copied perfectly and altered invisibly. In a physical exhibit, investigators can identify the object seized, its packaging and the persons who handled it. Digital evidence requires a comparable record of acquisition, preservation, transfer and examination.

A robust digital chain should record the source device or account, the date and time of seizure or acquisition, the person responsible for extraction, the method used to create forensic copies, relevant hash values, storage conditions, subsequent transfers, and every significant forensic action. Where cloud services or platforms are involved, investigators should document how the material was obtained and what information accompanied it.

Provenance should also extend to AI-generated material. If an investigator intentionally uses an AI reconstruction, enhancement or translation, that fact should be disclosed. A reconstruction may be useful for investigation or explanation, but it should not silently be converted into purported original evidence. The court should be able to distinguish the original file from a demonstrative or analytical output.

The principle is simple: the more transformative the technological process, the greater the need for transparency. Courts do not need to understand every algorithm mathematically, but they must know enough about the process to decide whether the resulting evidence can safely support a finding of fact.

## 6. Expert Evidence and the Role of Forensic Science

AI-related disputes will increasingly require expert evidence. The challenge, however, is to prevent a new form of 'expert authority' from replacing judicial reasoning. A forensic examiner should explain the method, limitations, data examined and basis for the conclusion. The court must remain the final decision-maker on admissibility and weight.

India already has a statutory concept of examiners of electronic evidence under Section 79A of the Information Technology Act. The future will require stronger institutional capacity: accredited laboratories, trained personnel, standard operating procedures, validated forensic tools, and transparent reporting formats. Expert reports should ideally distinguish between findings that are technically established and conclusions that remain probabilistic.

No AI detector should be treated as an infallible truth machine. Detection systems can produce false positives and false negatives, particularly as generative models improve. A responsible forensic opinion should therefore disclose the tool or methodology used, relevant error rates where known, the material examined, limitations, and whether independent methods support the conclusion.

Courts may also benefit from court-appointed neutral experts in technically complex cases, particularly where prosecution and defence experts reach sharply conflicting conclusions. Such mechanisms can help the judge understand the technology without transferring the judicial function to an expert.

## 7. Constitutional and Fair-Trial Concerns

The evidentiary problem is ultimately a constitutional problem. Article 21 of the Constitution protects life and personal liberty, and criminal procedure must satisfy the requirements of fairness and due process. A conviction based on fabricated digital material would strike at the core of these guarantees.

The accused must have a meaningful opportunity to challenge the evidence. This requires more than receiving a printed screenshot or a compressed video. Where authenticity is disputed, the defence may need access to the original file, relevant metadata, forensic reports, extraction details and, where legally permissible, information necessary to conduct an independent examination.

At the same time, privacy and proportionality concerns cannot be ignored. Digital investigations may involve enormous quantities of personal information. An investigation into one alleged offence can expose unrelated photographs, messages, location information and communications. The expansion of digital evidence should therefore be accompanied by careful controls on collection, access, retention and disclosure.

A fair-trial framework should also recognise equality of arms. Wealthier parties may have access to specialist forensic laboratories and technical consultants, while an accused relying on legal aid may not. If AI-generated evidence becomes common, access to competent digital-forensic assistance should become part of meaningful defence rights in appropriate

cases.

## 8. Should AI-Generated Evidence Be Admissible?

The answer should not be an automatic yes or no. AI-generated material can be relevant and sometimes highly useful. For example, an AI system might generate a visual reconstruction to explain a physical scene, translate speech, restore damaged information, or identify patterns in a large dataset. The fact that an output is AI-assisted does not by itself make it unreliable.

What matters is purpose and provenance. A reconstruction expressly presented as a reconstruction is fundamentally different from a fabricated video presented as an original recording. The first may assist understanding; the second may be deceptive evidence.

Indian evidence law is better served by a technology-neutral approach combined with strict authenticity safeguards. Courts should evaluate whether the material is relevant, whether its source and integrity can be established, whether the process used to generate or alter it is adequately explained, and whether its probative value is sufficiently reliable to justify reliance.

The court should also consider corroboration. A disputed synthetic video accompanied by independent CCTV footage, location records, witness testimony and device data presents a different evidentiary picture from a standalone anonymous video. Reliability should therefore be assessed holistically.

## 9. Proposed Safeguards for Indian Criminal Trials

First, courts should require clear disclosure whenever evidence has been generated, enhanced, reconstructed or materially altered using AI. Concealment of a material transformation should weigh heavily against the reliability of the evidence.

Second, investigative agencies should adopt standard digital-evidence protocols covering acquisition, hashing, preservation, documentation and access logs. Such protocols should be nationally consistent and regularly updated.

Third, forensic laboratories should develop specialised capacity for synthetic-media examination. This should include image, video and audio analysis, provenance assessment and evaluation of generative-model artefacts, while recognising that no single detection technique is universally reliable.

Fourth, procedural rules should facilitate defence access to the information reasonably necessary to test disputed digital evidence. This does not mean unrestricted disclosure of sensitive investigative material; rather, it means meaningful disclosure of material necessary to challenge authenticity.

Fifth, judicial education should be institutionalised. Judges need not become computer scientists, but they should understand the basic distinction between metadata, hashes, provenance, authentication, editing, generative synthesis and forensic inference.

Sixth, courts should distinguish original evidence from demonstrative evidence. An AI-generated reconstruction may be admitted for explanatory purposes without being treated as proof that the reconstructed event actually occurred.

Finally, legislation or rules should consider a specific framework for synthetic media used in judicial proceedings. The objective should not be to criminalise technology itself, but to make deliberate evidentiary deception easier to detect and harder to deploy.

## 10. Future of Criminal Trials in India

The future criminal trial will likely contain more digital material than physical exhibits. Investigators may rely on cloud records, connected devices, biometric systems, surveillance networks and AI-assisted analysis. Defence lawyers will increasingly need technical literacy, while prosecutors will need to establish digital provenance as carefully as they establish the chain of custody for a weapon or biological sample.

Artificial intelligence may also assist courts. Properly governed tools could help organise large records, identify inconsistencies, translate material or locate relevant portions of voluminous digital evidence. But decision-support technology must not quietly become decision-making technology. The ultimate judgment of guilt must remain with the legally authorised human court, applying legal standards to admissible evidence.

The most important shift may therefore be cultural. Courts should move from asking, 'Does this look real?' to asking, 'What is the evidentiary basis for believing that this material reliably represents what it claims to represent?' That question is more demanding, but it is also more compatible with the fundamental principles of criminal adjudication.

India's new criminal-law framework provides a useful foundation because it recognises digital records and technology-enabled procedure. The next step is to develop institutional practices capable of handling synthetic media. Without those safeguards, technological sophistication may increase the persuasive power of false evidence. With them, technology can strengthen investigation without weakening the presumption of innocence.

## 11. CONCLUSION

AI-generated evidence represents one of the most important emerging challenges for criminal justice. It does not make existing evidence law obsolete, but it exposes assumptions that were easier to maintain when creating a convincing photograph or voice recording required specialised equipment.

The Indian legal system should neither reject AI-generated material merely because it is artificial nor accept it merely because it appears authentic. The decisive questions should concern relevance, provenance, integrity, transparency, expert verification and the opportunity for effective challenge. The BSA, BNSS and the existing law relating to electronic evidence provide a statutory starting point, while judicial precedent supplies important principles concerning authentication and reliability.

The future of criminal trials will depend on preserving a balance. Investigating agencies need effective technological tools; victims need credible methods of proving offences; and accused persons need meaningful protection against fabricated or manipulated evidence. The answer lies in rigorous digital-forensic practice, transparent disclosure, independent examination and technologically informed judicial reasoning.

Ultimately, the courtroom must remain a place where evidence is tested rather than merely displayed. In an age in which artificial intelligence can manufacture persuasive realities, that principle may become more important than ever.

## REFERENCES

1. India Code, Bharatiya Sakshya Adhiniyam, 2023, especially Sections 61–63.
2. India Code, Bharatiya Nagarik Suraksha Sanhita, 2023, especially Sections 105 and 530.
3. Information Technology Act, 2000, Section 79A, India Code.
4. Anvar P.V. v. P.K. Basheer & Ors., (2014) 10 SCC 473.
5. Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal & Ors., (2020) 7 SCC 1.
6. Tomaso Bruno v. State of Uttar Pradesh, (2015) 7 SCC 178.
7. Supreme Court of India, judgments and official case materials concerning electronic evidence and proof.