INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 12 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

DEEPFAKES AND THE ADMISSIBILITY OF DIGITAL EVIDENCE: CHALLENGES UNDER INDIAN LAW

AUTHOR – SAHIL YADAV* & DR. AUSAF AHMAD MALIK**

* L.L.M. STUDENT, UILS, CHANDIGARH UNIVERSITY, MOHALI, PUNJAB, INDIA

** PROFESSOR, UILS, CHANDIGARH UNIVERSITY, MOHALI, PUNJAB, INDIA

BEST CITATION – SAHIL YADAV & DR. AUSAF AHMAD MALIK, DEEPFAKES AND THE ADMISSIBILITY OF DIGITAL EVIDENCE: CHALLENGES UNDER INDIAN LAW, INDIAN JOURNAL OF LEGAL REVIEW (IJLR), 6 (12) OF 2026, PG. 182-188, APIS – 3920 – 0001 & ISSN - 2583-2344.

ABSTRACT

Advances in artificial intelligence now allow anyone with the right tools to produce strikingly realistic audio, images and video showing people say or do things they never did. This kind of content, usually called a deepfake, causes trouble for evidence in two ways. A fabricated clip can be passed off as a genuine record, and a genuine recording can just as easily be waved away as machine-made. The second risk deserves real attention, because it erodes the probative value of authentic digital material and leaves courts unsure what to trust. This paper looks at how deepfake-related digital material is admitted and assessed under Indian law, focusing on the Bharatiya Sakshya Adhiniyam, 2023 (BSA). It studies Sections 61, 62 and 63 of the BSA, the role of expert opinion under Section 39, and the lasting relevance of the Supreme Court's rulings in Anvar P.V. v. P.K. Basheer and Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal. It also turns to the Information Technology Act, 2000 and the 2026 amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, keeping the regulation of online content separate from the question of judicial proof. The argument made here is that meeting the statutory requirements, including certification, may satisfy the conditions for receiving an electronic record, yet it does not settle whether the event shown really happened or whether the recording was synthetically altered. A dependable approach needs the original data to be preserved, a documented chain of custody, forensic examination proportionate to the dispute, expert evidence that explains itself, and a fair chance for the other side to challenge the material. The paper closes with recommendations for a technology-neutral and procedurally fair framework, one that shields courts from fabricated evidence without letting bare claims of manipulation undermine genuine recordings.

Keywords: Deepfakes; electronic evidence; Bharatiya Sakshya Adhiniyam, 2023; authentication; digital forensics; admissibility; expert opinion.

1. INTRODUCTION

Recordings of every kind now serve as everyday proof. CCTV footage, videos shot on phones, voice notes, chat records, photographs and files kept in the cloud can all help show where a person was, what

they did, what was said or how things stood at a given time. Yet this usefulness comes with a particular weakness. Digital content can be copied, edited, recompressed, re-encoded or even generated from scratch, and none of this leaves the visible traces that physical tampering used to leave. Artificial intelligence has made the weakness worse by making it possible to produce convincing audio-visual material that copies a real person's face, voice, gestures or way of speaking[564].

The legal worry goes beyond the spread of fake videos. Deepfakes can distort proof in both directions. In one case, fabricated content is offered to a court as a real recording in order to mislead it. In the other, a party who is faced with a genuine recording may be tempted to deny it by claiming, with no real basis, that it has been tampered with, simply because deepfake technology exists. This second problem is widely known as the 'liar's dividend', meaning that the mere existence of realistic synthetic media makes it easier to disown authentic evidence[565]. Either way, the reliability of adjudication is put at risk.

The paper asks whether Indian law gives courts enough protection against these challenges. Its main contention is that admissibility, authenticity and evidentiary weight are connected but separate questions. Following the statutory method for proving an electronic record is necessary, but it should not be mistaken for a scientific guarantee that the event shown in the recording is true.

2. RESEARCH PROBLEM, QUESTIONS AND OBJECTIVES

The core research problem is the distance between the traditional rules on electronic records and today's ability to create or alter lifelike synthetic audio-visual content. The BSA does recognise electronic and digital records. Still, deciding whether a given recording is genuine in practice may call for technical evidence that goes well beyond filing a statutory certificate. Three questions guide the paper. First, how does the BSA govern the admissibility of electronic records? Second, how should a court deal with a claim that a recording is a deepfake or has been manipulated? Third, which safeguards can stop fabricated material from being admitted while also stopping genuine evidence from being rejected without good reason?

The paper aims to analyse the statutory framework, study the relevant principles laid down by courts, point out the evidentiary risks that deepfakes bring, and propose practical safeguards that courts, investigators and litigants can use.

3. RESEARCH METHODOLOGY

The study follows a doctrinal and analytical method. It relies on the BSA, the Information Technology Act, 2000, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 as amended in 2026, and the relevant decisions of the Supreme Court of India. Secondary sources are used to explain the technical and evidentiary background of synthetic media. The work is qualitative, and it does not claim to have tested deepfake-detection tools empirically. The law is stated as it stood in November 2026.

[564] Nina Schick, Deepfakes: The Coming Infocalypse (Twelve, 2020). The term 'deepfake 'is used descriptively for realistic synthetic or materially manipulated audio-visual content.
[565] Robert Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security', 107 California Law Review 1753 (2019).

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 12 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

4. UNDERSTANDING DEEPFAKES AND THEIR EVIDENTIARY RISK

'Deepfake' is the common name for synthetic or manipulated audio-visual material that is produced or changed with machine-learning techniques so that it seems to show a real person or event. A deepfake might swap one face for another, imitate a voice, change lip movements, invent a whole scene, or blend real and synthetic elements. It can circulate as a full video, a short clip, an audio file, a screenshot or a re-uploaded copy. Not every digital edit amounts to a deepfake. Compression, cropping, brightness correction, noise reduction and format conversion all happen for ordinary reasons and often leave the substance of a recording untouched. What matters for evidence is whether a change materially affects the content, the context, who is speaking, the order of events or the meaning that is drawn from the record. Courts should therefore be careful not to treat every technical change as a sign of fabrication. In litigation, deepfakes pose at least four distinct risks. A fabricated recording may wrongly pin words or actions on someone. A genuine recording may be attacked as synthetic. An authentic recording may be edited selectively so that its context is distorted. And a genuine file that has been shared again and again across platforms may lose valuable metadata or its trail of origin. A forwarded or downloaded copy may simply not carry the information that the original device or source system holds.

5. THE INDIAN LEGAL FRAMEWORK FOR ELECTRONIC EVIDENCE

5.1 Sections 61, 62 and 63 of the Bharatiya Sakshya Adhiniyam, 2023

The BSA gives recognition to electronic and digital records. Section 61 says that such a record cannot be refused admissibility only because it is electronic or digital, although its legal effect remains subject to Section 63. Section 62 provides that the contents of electronic records can be proved in the manner set out in Section 63[566].

Section 63 deals with the admissibility of particular computer outputs. It lays down conditions about the regular use of the computer or communication device, the supply of information in the ordinary course, the proper functioning of the device, and the way the information was derived or reproduced. It also requires a certificate in the prescribed form, together with a Schedule. The Schedule asks for details of the source device or record, how the output was produced, and hash values[567]. These requirements matter because they help establish how the tendered output came into existence.

A Section 63 certificate, however, should not be read as a final finding that the scene or sound it relates to actually took place. What the certificate speaks to is the statutory conditions attached to the electronic record or computer output. It does not necessarily tell the court whether a face was synthetically swapped, a voice was cloned, a scene was generated, or the content was materially altered before it reached the device that produced the output. In a deepfake dispute, a court may therefore need further evidence on provenance, editing history and forensic indicators.

5.2 Expert opinion and electronic evidence

[566] The Bharatiya Sakshya Adhiniyam, 2023, Act No. 47 of 2023, ss. 61–62.
[567] s. 63 and the Schedule to the Bharatiya Sakshya Adhiniyam, 2023. The statutory certificate format includes source/device particulars and hash-value fields.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 12 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

Under Section 39(1) of the BSA, the opinion of a person with special skill in science, art or any other relevant field becomes a relevant fact where the court has to form an opinion on such a subject. Section 39(2) goes further and expressly treats as relevant the opinion of an Examiner of Electronic Evidence, as referred to in Section 79A of the Information Technology Act, 2000, where the court must form an opinion on information stored in or transmitted through a computer resource or other electronic or digital form[568]. This gives courts a statutory way of obtaining technical help in suitable cases.

Even so, expert evidence is not beyond error. A good report sets out what was examined, which methods and tools were used, where those methods fall short, what was found, and how confident the expert can reasonably be. Simply declaring that a video is 'AI-generated' or 'genuine' without giving reasons is of little use to a court. The opposing party must also be able to test the expert's assumptions, data, methods and conclusions.

5.3 Related criminal and intermediary regulation

The Information Technology Act, 2000 contains provisions that can apply to conduct linked with deepfakes, depending on the facts of a case. These cover identity theft, cheating by personation using a computer resource, violation of privacy, and the publication or transmission of certain obscene or sexually explicit material. The Bharatiya Nyaya Sanhita, 2023 may also come into play where the conduct meets the ingredients of offences such as cheating by personation or forgery, including the making of false electronic records[569]. Calling something a 'deepfake' does not, on its own, create criminal liability.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, notified as G.S.R. 120(E) and in force from 20 February 2026, brought in a framework for 'synthetically generated information'. Among other things, the amendments deal with labelling, traceability and the due diligence expected of intermediaries in relation to specified synthetic content[570]. These rules concern how synthetic media is created and circulated online. They leave untouched the separate job of the court, which is to decide whether a particular electronic record is admissible and how much weight it deserves in a proceeding.

6. JUDICIAL APPROACH TO ELECTRONIC EVIDENCE

In Anvar P.V. v. P.K. Basheer, the Supreme Court treated the statutory requirements governing secondary electronic evidence under Section 65B of the former Indian Evidence Act as mandatory. The Court held that electronic records tendered as secondary evidence had to satisfy the prescribed certification requirements[571]. The decision is important because it emphasises that electronic evidence cannot be admitted by disregarding the special statutory method for proving it.

In Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, a three-judge Bench reaffirmed the centrality of the Section 65B certificate for secondary electronic evidence and clarified the position

[568] s. 39(1)–(2); Information Technology Act, 2000, s. 79A.
[569] Information Technology Act, 2000, ss. 66C, 66D, 66E, 67 and 67A; Bharatiya Nyaya Sanhita, 2023, ss. 319 and 336. Applicability depends on statutory ingredients and facts.
[570] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, G.S.R. 120(E), Gazette of India, Extraordinary, Part II, s. 3(i), 10 February 2026 (effective 20 February 2026).
[571] 2014 10 SCC 473.

concerning its production and the role of the court in securing it where necessary[572]. The judgment discusses the rationale for statutory conditions governing computer outputs. These decisions interpreted the former Evidence Act. They remain relevant to understanding the background and principles of electronic-evidence certification, but must be applied carefully alongside the text of the BSA, which now governs relevant proceedings.

Neither decision dealt specifically with AI-generated deepfakes. Their principles nevertheless provide a starting point: the party relying on an electronic record must comply with the applicable statutory requirements. The additional problem raised by deepfakes is that procedural certification may not resolve the factual dispute over whether the content itself has been synthetically created or materially altered. Courts must therefore avoid equating formal admissibility with ultimate authenticity or reliability.

7. ADMISSIBILITY, AUTHENTICITY AND PROBATIVE WEIGHT: THREE DISTINCT QUESTIONS

Admissibility is about whether the material may lawfully be received in evidence. For a computer output, this means the conditions of Section 63 of the BSA have to be met. Authenticity is about whether the record is what the party says it is, for example an original CCTV export, an unaltered phone recording or a faithful copy of a source file. Probative weight is about how strongly the record supports the fact it is offered to prove, judged by its context, completeness, reliability and consistency with the rest of the evidence.

These three questions should be kept apart. A record can meet the formal requirements for admissibility and still be contested on authenticity or weight. The reverse also holds, since a bare allegation that a record is a deepfake should not exclude it automatically when nothing supports the claim. The court should look at how specific the challenge is, whether the source file is available, the chain of custody, the metadata, device records, witness testimony and any relevant forensic analysis. When a party alleges manipulation, the court should ask for more than guesswork. The challenger should point to a basis, such as an inconsistency within the recording, a gap in the chain of custody, signs of editing, a mismatch with the source device, or a credible preliminary forensic finding. The final burden of proof continues to depend on the applicable law and the issues in the case. This paper does not suggest a new rule that automatically shifts the burden merely because AI manipulation has been alleged.

8. PRACTICAL DIFFICULTIES IN DETECTING AND PROVING DEEPFAKES

To begin with, detection tools cannot be treated as final. How well they work can change with the method of generation, compression, resolution, length, language, background noise and any later editing. A detector can return false positives as well as false negatives. A court should not accept a numerical detector score as a legal conclusion without knowing how the tool was validated, how often it errs and where its limits lie.

Next, provenance is frequently weak. A clip that arrives through a messaging application may be several steps away from the device on which it was first recorded, and metadata can be stripped or changed along the way. Missing metadata does not by itself prove manipulation, and in the same way,

[572] 2020 7 SCC 1.

metadata that is present does not guarantee that the event shown actually took place. Chain of custody is another trouble spot, particularly when many people or systems handle the same material. Investigators should note who collected the device or file, when and where it was collected, how it was copied, what tools were used, where the original was kept and who had access to it. A cryptographic hash can show that a file stayed unchanged between two recorded points in its handling. What it cannot show is that the file was truthful or untouched before the first hash was calculated.

Lastly, there is a danger of leaning too heavily on expert evidence. Courts need to assess the reasoning and the material behind an opinion rather than simply defer to the expert's conclusion. The expert, for their part, should separate evidence of synthetic generation from ordinary editing, and should say so plainly where the available data is not enough for a reliable conclusion.

9. SUGGESTIONS FOR A MORE RELIABLE EVIDENTIARY APPROACH

To start with, investigators should keep the source device and the earliest available version of the recording wherever the law allows. A forensic image or verified copy should be made through documented procedures, and access to the original should be limited. The collection record should note the date, time, place, device details and the identity of whoever handled the material.

Then, the chain-of-custody record should run unbroken from collection until the material is produced in court. Hash values should be calculated at suitable stages and recorded along with the algorithm used, and the hash report should be kept together with the certificate and the other technical documents. It must also be described accurately. A hash helps compare the integrity of a file from the moment it was generated, but it says nothing about whether the depicted event is true.

Where a credible deepfake challenge is raised, the court should consider ordering a proportionate forensic examination by a suitably qualified expert, which could include an Examiner of Electronic Evidence where appropriate. The expert should be given the best source material available and should disclose the methods, tools, limitations and relevant findings. Both sides should get a fair chance to question the report and, if needed, the expert as well.

Courts should also give reasoned orders that are specific to the case. A challenge should not succeed merely because deepfake technology exists, and a recording should not be treated as beyond doubt merely because a certificate accompanies it. The court should state whether it is deciding admissibility, authenticity or weight, and name the evidence on which it relies for that decision.

Finally, judicial training and forensic capacity need attention. Judges, prosecutors, defence lawyers and investigating officers should understand basic ideas such as metadata, compression, source files, synthetic generation and hash verification. Public forensic laboratories should have validated tools and trained staff, and wherever a tool is used, its limits and validation should be open to scrutiny.

10. FINDINGS AND CONCLUSION

The discussion shows that Indian law already has a solid base for handling electronic evidence. Sections 61 to 63 of the BSA recognise electronic and digital records and set out a method for proving computer outputs. Section 39 allows expert opinion, including that of an Examiner of Electronic Evidence

under Section 79A of the Information Technology Act. The IT Act, the BNS and the amended IT Rules also deal with certain kinds of unlawful conduct and online circulation involving synthetic content.

Even so, these provisions do not remove the evidentiary difficulty that deepfakes create. Certification, platform labelling and forensic detection each do a different job. A Section 63 certificate does not conclusively prove that the depicted event occurred, a platform label does not decide admissibility, and the output of a detection tool cannot replace the court's own evaluation. The court has to weigh where the file came from and how it was handled, what kind of manipulation is alleged, how good the expert analysis is, and what the surrounding evidence shows.

The central recommendation is not to presume that digital recordings are unreliable, but to build a disciplined way of testing them. Such a method should guard against fabricated evidence, and at the same time prevent unsupported claims of AI manipulation from becoming an easy tool for discrediting authentic material. Whether digital evidence is trusted in court will turn neither on blind faith in technology nor on blanket suspicion of it, but on open procedures, dependable forensic practice and reasoned judicial scrutiny.

BIBLIOGRAPHY

Primary Sources

- The Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023).
- The Bharatiya Nyaya Sanhita, 2023.
- The Information Technology Act, 2000.
- The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended by G.S.R. 120(E), 10 February 2026.

Secondry Sources

- Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
- Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
- Chesney, Robert and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security', 107 California Law Review 1753 (2019).
- Schick, Nina, Deepfakes: The Coming Infocalypse (Twelve, 2020).