

DEEPPAKES AND EVIDENCE: CAN INDIAN COURTS TRUST DIGITAL MEDIA ANYMORE?

Reeti Nanda

O.P. Jindal Global University

ABSTRACT

In an age in which a video can be generated so realistically that seeing is no longer enough to establish truth, deepfake technology presents a serious challenge to the law of evidence. Indian courts increasingly rely on CCTV footage, mobile-phone recordings, photographs, voice notes, social-media posts and other electronic records to reconstruct disputed events. The Bharatiya Sakshya Adhiniyam, 2023 (BSA) recognises the legal status of electronic and digital records and, through Sections 61–63, provides a framework for their proof. Yet the statutory framework is primarily concerned with the admissibility, preservation and procedural certification of electronic records. Deepfakes expose a further problem: a file may be intact, accurately copied and validly certified, while the event depicted in it may never have occurred. This article therefore argues that Indian courts should distinguish between the integrity of a digital file and the authenticity of the reality it purports to represent. It proposes a five-stage judicial framework Admissibility, Integrity, Authenticity, Provenance and Substantive Corroboration (AIAPS) for cases in which electronic media is alleged to be AI-generated or manipulated. The framework requires judges to determine whether the record is legally admissible, whether it has remained unaltered, whether it accurately represents an event, whether its origin and chain of custody can be established, and whether independent evidence supports the substantive proposition for which it is tendered. The article further considers whether Section 63(4) BSA can be judicially interpreted to meet the deepfake problem or whether legislative intervention is eventually necessary, while accounting for India's practical constraints, including limited forensic capacity, chain-of-custody failures, judicial workload and unequal access to technical expertise.

KEYWORDS: Deepfakes, Digital Evidence, Electronic Evidence, Artificial Intelligence, Bharatiya Sakshya Adhiniyam, 2023, Authentication, Digital

INTRODUCTION

Indian courts have increasingly relied on digital evidence to be able to reconstruct events and to establish disputed facts. Evidence from CCTV footage, mobile phones, photographs, voice notes and content from emails can be useful on what happened.¹ Content from emails, voice notes, photographs, mobile phone and CCTV footage may inform on what happened. But generative AI has thrown a curveball at a fundamental assumption in evidence: that a recording must reflect an actual event.² Audiovisual material can be created or altered so imperceptibly by deepfakes that it is no longer possible to tell if it is real or fake by simply looking at or listening to the imagery.

The problem is not as simple as normal editing. Traditional authentication is usually asking the question of whether a recording has been interfered with since it was made. Instead, a deepfake could be the synthetic representation from the start. If this occurs, however, there could be no “original event” to which the recording refers. The question of evidence thus becomes not whether this file has been tampered with, but what does this file reliably prove (what has it not proven, either?).³

This is important to make under the Bharatiya Sakshya Adhiniyam, 2023. An electronic or digital record shall not be disallowed because it is electronic or digital in accordance with Section 63, except in the case of records under Section 61. Section 62 discusses proof of the contents of an electronic record, and Section 63 discusses the conditions under which electronic records will be proved and incorporates a certificate that includes the device/source information and a hash value, along with expert certification. The statutory requirements enhance the procedural protections, but a certificate does not in itself prove that the event shown actually took place in physical reality.⁴

The article thus calls for a multilayered approach. The mere existence of deepfakes should not discredit the use of electronic evidence in court. Nor may they assume a role of substantive truth from the mere fact of statutory certification. Rather, a structured judicial test is to be applied, which distinguishes the admissibility of evidence, integrity, authenticity, and

¹ Bharatiya Sakshya Adhiniyam 2023, ss 56–63.

² Anvar PV v PK Basheer (2014) 10 SCC 473

³ Bharatiya Sakshya Adhiniyam 2023, ss 39(2), 40, 45.

⁴ Bharatiya Sakshya Adhiniyam 2023, s 39(2).

provenance and substantive corroboration, where there is a credible allegation of synthetic manipulation.

MECHANICS OF SYNTHETIC DECEPTION: TECHNOLOGICAL AND EVIDENTIARY RISKS

Deepfakes are synthetic or manipulated AV materials created or modified using machine learning.⁵ These can include facial reconstruction, voice cloning, lip synchronization manipulation and complete synthetic voices. In the early days, the systems for creating deepfakes were often referred to as Generative Adversarial Networks, but today, there are other architectures for generative systems that are also in use. The law issue is not limited to any specific technology but can be caused by the capacity to make a convincing media that represents identity, speech, conduct or context.

Three risks are of special concern from an evidentiary perspective. The first is fabrication: a completely imaginary recording is used to portray a person doing or saying something that could not have actually occurred. Secondly, a genuine recording can be manipulated, for example by replacing a face/voice. Thirdly, the "liar's dividend" principle means that evidence truly produced by the AI could be discarded simply because a party argues it is AI-generated!

All these risks illustrate that this visual authenticity test is not sufficient. Metadata might be incomplete or even be removed; files are often recompressed by social media platforms; screenshots can lose out on context; and advanced synthetic media can lack the tell-tale signs of standard editing. A court will thus look at the record as a whole and not at the record file in isolation.⁶

Your One Stop Legal Destination

THE STATUTORY FRAMEWORK: FROM SECTION 65B OF THE IEA TO SECTIONS 61–63 BSA

The law with respect to electronic evidence has come from Bharatiya Evidence Act, 1872 to Bharatiya Sakshya Adhiniyam, 2023. The old framework for proving electronic records was

⁵ Chesney and Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753.

⁶ Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1.

provided by Sections 65A and 65B.⁷ *State (NCT of Delhi) v Navjot Sandhu*, *Anvar P.V. v P.K. Basheer and Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* were the Supreme Court decisions that laid the foundation for the concept of certifications and secondary electronic evidence as it is understood today.

Section 61 BSA provides that an electronic or digital record shall not be excluded simply because it is in electronic or digital format, and apply Section 63 to it.⁸ Section 62 makes it clear that contents of electronic records may be proved pursuant to Section 63.⁹ Section 63 sets out the requirements for adducing electronic records and, for the applicable category, a certificate pursuant to Section 63(4).¹⁰ The statutory Schedule asks for details about the device or source, how the record was created and the hash of the record; Part B also assumes that the expert will certify the record.¹¹

The new certificate is meaningful because the hash value is like a “fingerprint” for a specific file. It can be used to show that a file presented in court was actually the same file that was hashed at the appropriate time. You can get technical assurance from expert certification. The Supreme Court in *Pune Bar Association v Union of India* (2026) upheld the constitutional validity of Section 63(4), emphasising the rational connection between hash values, expert certification and the objective of ensuring the authenticity and integrity of electronic records. The Court further clarified that the detailed definition of “expertise” as detailed in the Examiner of Electronic Evidence by the Madras High Court, which was proposed under Section 79A of the Information Technology Act, should not be considered as a binding precedent and the exact scope of the expertise should be left open based on an appropriate case.¹²

Your One Stop Legal Destination

But the key restriction is cognitive. A hash is used to check the authenticity of a digital object at a given moment in time, not the veracity of the story it tells. Likewise, the testimony of an expert who certifies or testifies to the technical features of a device or file may be used to establish that the file was correctly extracted and preserved, but does not necessarily establish

⁷ Indian Evidence Act 1872, ss 65A–65B.

⁸ Bharatiya Sakshya Adhiniyam 2023, s 61.

⁹ *ibid*, s 62.

¹⁰ *ibid*, s 63.

¹¹ *ibid*, s 63(4) and Schedule.

¹² Information Technology Act 2000, s 79A

that the visual event shown actually took place. A well-preserved deep fake is a well-preserved deep fake.

Therefore, it should be considered that Section 63(4) is not a full deepfake-authentication mechanism. It's a large portion of the chain between source to the courtroom, but not the entire epistemic question of if the content is real.

JUDICIAL TRAJECTORY AND THE DEEPPFAKE BLIND SPOT

From Navjot Sandhu to Anvar P.V.

In *State (NCT of Delhi) v Navjot Sandhu*, the Supreme Court adopted a comparatively flexible approach to electronic evidence.¹³ The later decision in *Anvar P.V. v P.K. Basheer* rejected that approach and treated Sections 65A and 65B as a specialised statutory code for secondary electronic evidence.¹⁴ The Court emphasised certification as a safeguard against unreliable electronic material.¹⁵

Arjun Panditrao Khotkar

A three judge Bench in *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* again emphasized the importance of the Section 65B certificate for secondary electronic evidence and explained the difference between original electronic evidence and copies.¹⁶ The judgment also held that the “procedural requirements” should not be imposed in the impossible way.¹⁷ The judgment is crucial for electronic evidence, and precedes the vast problem before the courts of generative synthetic media.

The deep fake blind spot, then, is not to be taken as Arjun Panditrao is incorrect. Instead, both "procedural question" and "deepfake question" are different. A certificate can create the documentation of the production and preservation of a copy. It can't determine if the person depicted actually committed the act, if the voice was actually that person's, or if the scene itself was created by AI.

¹³ *State (NCT of Delhi) v Navjot Sandhu* (2005) 11 SCC 600.

¹⁴ *Anvar PV v PK Basheer* (2014) 10 SCC 473.

¹⁵ *ibid.*

¹⁶ *Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.

¹⁷ *ibid.*

PUNE BAR ASSOCIATION: WHAT SECTION 63(4) CAN AND CANNOT DO

Pune Bar Association V Union of India is especially relevant to the case as it holds that the safeguards embedded into Section 63(4) are valid.¹⁸ The Supreme Court acknowledged the significance of hash values and expert certifications, and considered them to be rational protections, not random impositions. This enhances the procedural framework of electronic evidence. It is not, however, a substantive finding of authenticity based on procedural certification.

A more generous reading of section 63(4) is, therefore, to be taken as a minimum rather than a maximum. Compliance should make the court satisfied that the electronic record has moved past the threshold for consideration. If the record is specifically claimed to be fabricated, then the court has the general powers of evidence law to call for expert opinion, review the source and chain of custody, compare the media with independent records, and determine if the substantive fact asserted is corroborated. This is not a rewrite of Section 63, but it helps to avoid the confusion that the Section 63 would otherwise cause if it were taken to be a complete truth verification rule.

A PROPOSED JUDICIAL FRAMEWORK FOR SUSPECTED DEEPPAKES

Indian courts require a practical test that can be applied without turning every digital-evidence dispute into a full technological trial. This article proposes a five-stage framework: Admissibility → Integrity → Authenticity → Provenance → Substantive Corroboration (AIAPS). The stages should be treated as sequential but interconnected. A court may stop at an earlier stage if the evidence fails there; conversely, passing one stage should not create a presumption that the later stages are satisfied.¹⁹

Your One Stop Legal Destination

Stage 1: Admissibility

The first question is whether the material is legally admissible to be received in evidence. The court should determine if the record is primary or secondary electronic evidence and if the requirements of the BSA, especially Section 63 and the certificate requirements of the BSA, have been met.²⁰ The court also needs to designate the specific fact about which the record

¹⁸ Pune Bar Association v Union of India, 2026 SCC OnLine SC 551.

¹⁹ Pooja Singh, 'Digital Forensics and Electronic Evidence in India: Admissibility, Integrity and Due Process under the Bharatiya Sakshya Adhiniyam, 2023' (2026) *Indian Journal of Law and Legal Research*, Volume VIII Issue II.

²⁰ Bharatiya Sakshya Adhiniyam 2023, ss 3, 4, 61–63.

will be submitted. A video could be allowed as evidence that a file was uploaded at a given time, but without being necessarily reliable evidence that the event depicted in the video was the event itself.

Stage 2: Integrity

The second question is whether the particular digital file has remained unchanged from the point of collection to its production in court. The judge should consider hash values, extraction methods, storage media, device imaging, metadata, preservation procedures and the chain of custody. Where a social-media download is relied upon, the court should ask whether the platform has recompressed or transformed the material and whether the version tendered is the same version originally published. Integrity is therefore about the identity and preservation of the digital object.

Stage 3: Authenticity

Authenticity does not ask the question of whether the recording is accurate as to the person, event, sound or scene it claims to represent, but whether it actually does. When a party claims that a video was created by AI, the court should not make the determination without viewing the video. Forensic analysis of frames and sounds, compression artefacts, inharmonicities in facial and vocables, lighting and shadow analysis, temporal continuity, generation traces, metadata and other scientifically recognized indicators should be taken into account, depending on the circumstances. If the question is outside the common knowledge of the court, the court should seek expert advice.²¹

Importantly, a court should not require certainty from a forensic tool just because it provides an “AI detector” output. Detection tools may have false-positive and false-negative rates and may be outdated due to advancing generative technology. Expert evidence needs to not only provide a percentage score, but also include information about the methodology, limits, reliability and basis of the conclusion.

Stage 4: Provenance

Provenance asks where the content came from and how it travelled to the courtroom. The court should identify, as far as reasonably possible, the original device or platform, the

²¹ Zohaib Ahmed, ‘How to Authenticate an Audio Recording That Sounds Real’ (Resemble AI, 10 February 2026) <https://www.resemble.ai/resources/authenticate-audio-recordings-evidence> accessed 12 September 2026.

creator or uploader, the date and circumstances of creation, the persons who handled the record, the transfer history, and any transformations such as editing, compression or conversion. Where available, original device data, platform records, server logs, cloud records, contemporaneous messages and independent copies should be examined. Provenance is especially important because a file can be technically intact while its source remains unknown or its context is misleading.²²

Stage 5: Substantive Corroboration

The final and most crucial question is what is the independent evidence that backs up the proposition for which the video is being used? The court can take evidence from other cameras (CCTV), access control records, location data, transaction records, contemporaneous communications, witness evidence or objective material if a video is supposed to show a person at a specific location. If the video is supposed to be a recording of a statement, the court may consider whether the statement is consistent with the facts which are independently established or with other contemporaneous evidence.

This is a stage where technical authentication cannot be used as substantive proof by the court. A video may be a true digital object, but it may also be misleading due to the lack of context. On the other hand, even if the digital file is not accepted as genuine, a serious event could be verified by several independent sources. The final job of the judge is not just to certify a file, but to evaluate the proposition that a party seeks the file to substantiate.²³

WHAT SHOULD A JUDGE DO WHEN A PARTY ALLEGES THAT A VIDEO IS AI-GENERATED?

The proposed framework may be put into practice through a practical courtroom protocol. First, the judge should ask the party objecting to specify the basis of the allegation, not leave it to the party to make a “mere” assertion that “AI could have made this”. Second, the court should retain the disputed file as it is submitted to them, record the hash value of the file (if suitable) and not allow it to be downloaded multiple times or edited so as to lose its provenance. Thirdly, the court should determine if the dispute is about the integrity of the

²² United Nations Development Programme, *Human Development Report 2025: A Matter of Choice—People and Possibilities in the Age of AI* (2025) <https://hdr.undp.org/system/files/documents/global-report-document/hdr2025reporten.pdf> accessed 13 September 2026

²³ Diganth Raj Sehgal, ‘Admissibility of CCTV Recordings as Evidence in Courts’ (iPleaders, 29 May 2021) <https://blog.iplayers.in/admissibility-cctv-recordings-evidence-courts/> accessed 15 September 2026.

file, the identity of the person in the file, whether the event is depicted, or the context in which the content of the file is presented.

Fourthly, where the allegation has a reasonable evidentiary basis, the court should direct a focused forensic examination. The expert MUST receive the original or forensically acquired material and not just a compressed screen shot or screen recording of better material.²⁴ The methodology used should be described by the expert, as should be the limitations of the analysis and the amount of confidence he/she should have based on the evidence. Fifthly, the court should allow the other party to examine the expert finding as well as, if relevant, provide their own expert materials.

Finally the judge should get back to the substantive fact in issue.²⁵ The court should inquire into whether, despite being technically authentic, the media establishes the proposition for which it is offered. Where the evidence is genuinely uncertain, there should be appropriate weighting of the evidence. In criminal proceedings, it should work in line with the prosecution's burden of proof beyond reasonable doubt; in civil proceedings, the burden of proof requirement to be applied should be consistent with the applicable burden of proof.

This method is also safe from the other risk: “liar's dividend”. A party shouldn't be able to defeat reliable evidence simply by asserting the possibility of the creation of a deep fake. The allegation process should result in proportional verification, not automatic rejection of the evidence.

CAN SECTION 63(4) BSA BE JUDICIALLY INTERPRETED, OR IS LEGISLATIVE AMENDMENT NECESSARY?

The quick response is that judges can do much but they can't fix all the elements of the deepfake issue. It is reasonable to interpret Section 63(4) as requiring procedure to be followed on electronic records with room for the courts to decide on authenticity and weight. There is also a statutory duty to accept specialised technical assistance in Section 39 BSA which recognises expert opinion. The Supreme Court's rationale in Pune Bar Association

²⁴ National Institute of Standards and Technology, *Digital Investigation Techniques: Forensic Examination of Digital Evidence* (NIST).

²⁵ Bharatiya Sakshya Adhinyam 2023, ss 3–4.

strengthens the value of experts, but does not provide clarity as to what types of experts are qualified to be part of the class.

But there's a limit to interpretation. There are no specific requirements for determining authenticity of a deepfake, minimum standards for conducting forensics of synthetic media, disclosure requirements regarding the manipulation of synthetic media, nor a single set of procedures to maintain synthetic-media evidence in the BSA. Nor does there seem to be any particular wording in Section 63(4) to require the certifier to explicitly state that the content was not AI-generated.²⁶ These stipulations can be challenging to impose on the statutory language without effectively 'judicially creating' new legislation.

So, the best scenario is a two-stage action of response. In the short term, courts should interpret the sections of this Act, as well as the general evidentiary principles, harmoniously, and view procedural certification as a condition that must be met if applicable, but not as substantive proof of substantive truth. In the longer-term, it is imperative that any Parliament and/or the rules-making bodies reconsider a relevant amendment or procedure regarding synthetic media. Preservation of original files, documentation of hash values, chain-of-custody, disclosure of known transformations, access to qualified digital-forensic examination, and a way to challenge expert testimony are likely to be required for such reform.

The law should also not make section 63(4) such that it makes it impractical for the typical litigant to produce digital evidence. Protections or lack of them and ease of access are demonstrated by the Pune Bar Association. The fact that a deepfake regime has to be examined on a case-by-case basis for each WhatsApp video would bring an overwhelming burden on both parties and courts. Thus, there needs to be a real clash, the importance of the evidence, and the fact that it is digital evidence and can be manipulated or has been manipulated could affect the result, not just that it's digital evidence.²⁷

²⁶ Bharatiya Sakshya Adhiniyam 2023, s 63(4).

²⁷ Mayank Makhija and Naman Sharma, 'Unseen Burden Of Electronic Evidence' (LiveLaw, 21 August 2026) <https://www.livelaw.in/articles/unseen-burden-electronic-evidence-546749> accessed 14 September 2026.

INDIAN PRACTICAL REALITIES: THE AUTHENTICATION GAP

If the judiciary is to become a reality it must be reflected in a judicial framework. In India, the trial courts frequently encounter electronic evidence in the absence of any specialised digital-forensic laboratories or experts. Forensic facilities are often spread over a large area, and may be overloaded, making it hard to obtain a prompt examination. Delays in forensic reporting can extend trials in criminal cases, and in civil and commercial disputes, the cost of private forensic examination can cause access to expertise to be unequal.

Another challenge are chain-of-custody issues. Evidence can go through investigating officers, police stations, forensic labs, attorneys, storage devices and court registries. Contents of your social media could be downloaded by different people at different times. Files can be compressed, renamed, converted or copied, but not documented. A sophisticated legal standard is little more than a fanciful concept without any evidentiary support.

The workload of judges needs to be taken into account as well. Trial judges are not expected to be experts in machine learning or in analysis of audiovisual forensics and metadata. The answer is not for judges to bear the burden of technology, it is to establish a process for judges to find the proper technical question or to get understandable expert help. The burden could be greatly alleviated with the use of standardised forensic protocols, accredited laboratories, trained court-appointed experts and short explanatory technical reporting.

The threat of unequal justice is also present. Wealthier parties can hire a number of experts and more advanced forensic reports, whereas individual litigants might not be able to afford these. This is because courts should continue to have the power to serve reasonable directions for the production of an independent qualified expert when the issue is material, and not require the truth of electronic evidence to be established in the way of a litigation budget.

All these pragmatic considerations strengthen the argument for proportionality. Not all low stakes digital records require the same level of attention. If there is a question of who is who, who had consented and who did not, who was criminal or not, who had a right to public safety or not, who had a right to a finding or not, then enhanced verification should be considered essential.²⁸

²⁸ Neha Haldhar, 'Electronic Evidence and Its Admissibility in Indian Courts' (B&B Associates LLP, 2026) <https://bnblegal.com/article/electronic-evidence-and-its-admissibility-in-indian-courts/> accessed 17 September 2026

RECENT INDIAN JUDICIAL EXPERIENCE WITH SYNTHETIC MEDIA

The developing judicial response to deepfakes also demonstrates that courts are already confronting harms arising from synthetic media outside the traditional evidence-law setting. In *Sudhir Chaudhary v Meta Platforms Inc.*, the Delhi High Court dealt with allegedly AI-generated videos using the plaintiff's name, image, likeness and voice.²⁹ The Court granted interim protection and directed removal of specified content. The order illustrates an important distinction: in urgent civil proceedings, a court may need to prevent continuing harm before a full forensic determination can be completed.

The case also demonstrates why preservation matters. Where synthetic media is being circulated rapidly, removal may prevent harm but can also risk loss of evidence. Courts should therefore consider preservation directions alongside takedown or protective orders where the material may be relevant to future adjudication. The objective should be to stop continuing harm without destroying the evidentiary trail needed to determine responsibility.

CONCLUSION

Deepfakes don't make digital evidence unusable. These are inaccurate common misconceptions about digital evidence. Indian courts must not shift from the “seeing is believing” mantra to the “nothing digital can be trusted” mantra. Neither of these is a good option. The right way to go about this is to be increasingly specific in asking what a digital record is evidence of.

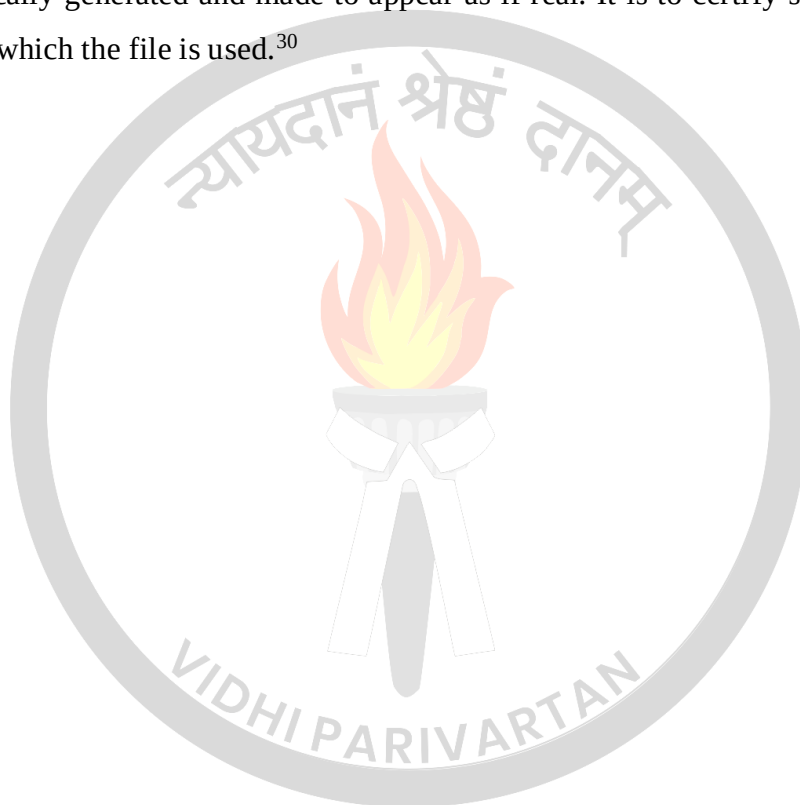
The procedural underpinning is important in Sections 61-63 of the BSA. Section 63(4), especially in the context of *Pune Bar Association v Union of India*, provides substantial protections, such as source information, hash values and expert certification. But these safeguards primarily address the identity, preservation and production of the electronic record. They do not definitely prove what occurred in the event shown. The law must thus separate the admissibility, integrity and substantive authenticity.

The proposed AIAPS framework (Admissibility, Integrity, Authenticity, Provenance, Substantive Corroboration) provides a feasible way to achieve this. It provides judges with a way to reply proportionately if a deep fake allegation is brought, saves the purpose of

²⁹ *Sudhir Chaudhary v Meta Platforms Inc.*, 2025 SCC OnLine Del 10572

authentic electronic evidence, and avoids a valid certificate being a 'short cut to truth'. It also protects against the liar's dividend: it 'screws' the liar in that they should have a reasonable basis for casting their vote before it gets singled out for heightened scrutiny.

What is the question here is not whether Indian courts can trust digital media, but how? Instead, it seems the more useful question to ask is whether courts can identify what a specific digital record actually proves in a transparent and proportionate way. The task of the judge is no longer just to verify that the file is genuine, since there are times when such files can be synthetically generated and made to appear as if real. It is to certify such evidentiary proposition for which the file is used.³⁰



Your One Stop Legal Destination

³⁰ *Bharatiya Sakshya Adhiniyam 2023* ss 61–63.