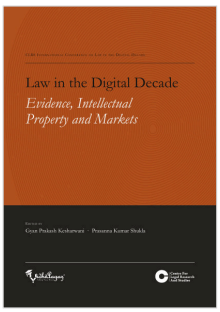
vidhiaagaz.com | support@vidhiaagaz.com

CHAPTER 4

When Seeing Is No Longer Believing: Deepfakes, Synthetic Evidence and the Criminal Process in India

Shirvi Goyal



in *Law in the Digital Decade: Evidence, Intellectual Property and Markets*, edited by Gyan Prakash Kesharwani and Prasanna Kumar Shukla (VidhiAagaz 2026), pp. 31–40

DOI https://doi.org/10.63108/VAB.LDD.2.4

CITATIONS

BLUEBOOK (21ST ED.)
Shirvi Goyal, *When Seeing Is No Longer Believing: Deepfakes, Synthetic Evidence and the Criminal Process in India*, *in* LAW IN THE DIGITAL DECADE: EVIDENCE, INTELLECTUAL PROPERTY AND MARKETS 31 (Gyan Prakash Kesharwani & Prasanna Kumar Shukla eds., VidhiAagaz 2026).

OSCOLA (4TH ED.)
Shirvi Goyal, 'When Seeing Is No Longer Believing: Deepfakes, Synthetic Evidence and the Criminal Process in India' in Gyan Prakash Kesharwani and Prasanna Kumar Shukla (eds), *Law in the Digital Decade: Evidence, Intellectual Property and Markets* (VidhiAagaz 2026) 31.

CHICAGO (17TH ED.)
Goyal, Shirvi. "When Seeing Is No Longer Believing: Deepfakes, Synthetic Evidence and the Criminal Process in India." In *Law in the Digital Decade: Evidence, Intellectual Property and Markets*, edited by Gyan Prakash Kesharwani and Prasanna Kumar Shukla, 31–40. Maihar: VidhiAagaz, 2026. https://doi.org/10.63108/VAB.LDD.2.4.

APA (7TH ED.)
Goyal, S. (2026). When seeing is no longer believing: Deepfakes, synthetic evidence and the criminal process in India. In G. P. Kesharwani & P. K. Shukla (Eds.), *Law in the digital decade: Evidence, intellectual property and markets* (pp. 31–40). VidhiAagaz. https://doi.org/10.63108/VAB.LDD.2.4

SOURCE

https://doi.org/10.63108/VAB.LDD.2.4

LICENCE

Open access under the Creative Commons Attribution-NonCommercial 4.0 International Licence (CC BY-NC 4.0): it may be copied, shared and adapted for non-commercial purposes, with credit to the authors and the source.

Citations are given as a guide; check them against the style manual you follow. This page was added by VidhiAagaz to the downloaded file. The chapter follows, with the page numbers of the printed book.

Law in the Digital Decade: Evidence, Intellectual Property and Markets, edited by Gyan Prakash Kesharwani and Prasanna Kumar Shukla (VidhiAagaz 2026) · Open access under CC BY-NC 4.0 · https://doi.org/10.63108/VAB.LDD.2.4

CHAPTER 4

When Seeing Is No Longer Believing: Deepfakes, Synthetic Evidence and the Criminal Process in India

SHIRVI GOYAL*

Deepfakes and similar technologies of synthetic media can generate such accurate images, videos, and audio, as to convincingly replicate real people and events. Although the technology might be utilized in crimes, such as fraud, identity theft, and image-based abuses, it poses a significant challenge to the role of digital evidence. The present paper discusses the likely and emerging challenges which deepfakes and synthetic media may present to criminal process in India. It interrogates whether the present law governing electronic evidence, including under the recently enacted Bharatiya Sakshya Adhiniyam, 2023, provides sufficient framework to deal with the issues of integrity, authenticity, and reliability that emerge from AI-generated or synthesized material. It argues that standard methods for electronic evidence may fail if issues related to the veracity of the recorded content are in conflict with the reliability of its preservation. Finally, the study addresses the role of forensic analysis, metadata and digital provenance in differentiation of true recordings from the synthesized. It evaluates the risk of the "liar's dividend" where authentic evidence can be disregarded because of readily available manipulation technologies. The research will conclude by recommending greater procedural and evidentiary protections that will allow criminal justice process to react to synthetic evidence without discrediting authentic digital recordings.

Keywords: Deepfakes; Synthetic Evidence; Digital Evidence; Criminal Process; Electronic Evidence.

1 INTRODUCTION

It is difficult not to assume that digital evidence will form a central feature of the criminal justice system moving forward. Records that may once have been overlooked by authorities, such as CCTV footage, mobile-phone records, photographs and messages are now routinely used as part of investigations and to prove charges in courts. These concerns were formally recognized by the Bharatiya Sakshya Adhiniyam, 2023, hereinafter the "BSA", giving these electronic and digital records the same status in law as documentary evidence, subject to their conditions of admissibility being met.[1]

This raises a new issue of the challenges presented by 'deepfakes'. Unlike standard digital records, a video may not actually reflect the event, or an image may not have been faithfully captured. They raise evidentiary problems in that such synthetic material may contain any statement made by anyone, and could result in evidence being wrongly taken that the defendant made or did whatever the relevant communication alleges. In many cases this is significant only in so far as it goes to establishing the individual identified as the defendant and what conduct they are alleged to have undertaken.

Indian courts, including the Supreme Court, have always treated electronic evidence very differently. In 2020, the Supreme Court re-affirmed many of these principles by emphasizing compliance with the strict statutory rules for proving electronic records as enshrined in the (then) Indian Evidence Act in a

* Student at Law College Dehradun, Uttaranchal University, Dehradun, Uttarakhand, India.

[1] Bharatiya Sakshya Adhiniyam, 2023, §§ 61–63.

landmark case called *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*.[2] Whilst a new act has been put into place called the BSA it has retained specific parts relating to the authenticity, and admissibility of digital evidence. This compliance with technical regulations does not, however, make the content genuine and could result in the introduction to court of manipulated or synthetic content even though it does, under specific provision of the BSA fit the rules relating to admissibility of digital evidence as previously provided for.[3]

Criminals have always sought to perpetrate fraud against others through some method of manipulating real evidence in order to get persons to comply with whatever demands are made. While this is now achieved through new technologies, deepfakes create a two-prong attack, against individuals through both use in fraud or image-based abuse, as well as against the idea of individual guilt. An attack on both can make existing evidence seem more realistic, while in fact causing the opposite: where courts, witnesses or evidence purveyors might begin dismissing genuine audio-visual recordings as synthetic based on the mere fact that technically manipulation is possible – 'the liar's dividend.'[4]

This paper discusses the impact of deepfakes on the Indian criminal process. It explores the existing framework relating to digital evidence and focuses upon the evidentiary challenges of authenticating the integrity of synthetic data in investigations and in court. It is argued that while admissibility regulations have a role, the primary challenges lie in the forensic ability to prove what evidence is and is not synthetically generated.

2 DEEPFAKES AND THE EMERGING LANDSCAPE OF CYBERCRIME

2.1 Nature and Uses of Deepfake Technology

The deepfake represents a category of synthetic media that use an AI's manipulation or addition of visual or sonic components to someone's image or voice to generate an audiovisual recording where such a person appears to say or do something that didn't in fact happen. The issue the technology creates involves not just the manipulation of digital records, but the very increasing ability of such technology to produce an event that seems completely true to a user without expertise. Such technology has transformed from being exclusive to technically capable people to publicly available online.[5]

2.2 Deepfakes and Emerging Forms of Cybercrime

Criminal activity using deepfakes follows the spread of this accessibility. One application has already arisen under fraud and impersonation. Synthetic audio or video material may attempt to replicate a real person to imitate a communication and create the effect of reality. Such an event may prove advantageous within social engineering, directed fraud, impersonation-based deception, and other forms of financial cybercrime. An instance the FBI reported where this occurred included use within personalized social engineering schemes, spear-phishing attacks, business email compromise and similar fraud actions.[6] Such an advantage would become considerably amplified where a participant in a criminal transaction views

[2] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
[3] Bharatiya Sakshya Adhiniyam, §§ 61–63.
[4] Bobby Chesney & Danielle Keats Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 CALIF. L. REV. 1753, 1785–86 (2019).
[5] FED. BUREAU OF INVESTIGATION, OVERSIGHT OF THE FBI CYBER DIVISION (Mar. 29, 2022).
[6] *Id.*

realistic visual or acoustic representations that seem to be evidence familiar to them from past occurrences, inducing trust without further evaluation.

Serious risk has also been developed for sexual assault, harassment and sextortion. A person's photographs or video taken earlier in a relationship or publicly available online can be altered to seem like the victim engaged in a sexual act. Subsequently the individual will be threatened with the publication of such an event, or be forced into providing cash or real sexual encounters. There are instances where minors, as well as adults, have become targets of deepfake images to facilitate sexual violence, extortion or other criminal acts.[7] Such consequences can, without true sexual content, be brought about by mere images depicting it.

Another area of concern is false attribution and identities. A synthetic performance might appear to record an individual at any specific time saying they did something that they hadn't, or being at a specific place when he or she wasn't. This is especially problematic when an individual may view fake material prior to evidence collection efforts being in place. Once distributed, fake images may impact many in the public sphere before their authenticity is verified.

2.3 The Liar's Dividend and Threats to Digital Evidence

Deepfakes present a problem in that people aren't just viewing evidence that is manipulated; they might find their own future use of a real image challenging where proof of that authenticity isn't easily established. This represents something more than another avenue for fraud – there is a potential challenge with verifying every digital piece of data for authenticity.[8] The FBI acknowledges this problem has and will lead to questions surrounding how to establish authenticity when looking at real digital evidence. The risk of deepfakes becomes even greater when looking at their role in the evidentiary process. An unauthentic performance of a crime may at first view be assumed as genuine traces leading an investigation. On the other hand, parties might attempt to challenge authentic visuals or acoustic performances as deepfakes, thereby introducing questions of how real footage ought to be used as proof. These issues need to be anticipated and considered as these technologies gain access throughout India. An increased access will force Indian judicial proceedings to take account of deepfake technology, thereby allowing for either their use within the fraudulent context, or demanding stricter standards for evidence.

3 Digital Evidence within the Indian Criminal Justice Landscape

3.1 Legal Framework for Electronic and Digital Evidence

The Indian criminal justice system has, to some extent, moved beyond the traditional notion that evidence is primarily composed of physical documents and oral testimony. Electronic evidence has become an inherent part of criminal investigation and trial, owing to the ubiquitous nature of mobile phones, computers, cloud storage, and digital communication systems. The Bharatiya Sakshya Adhiniyam, 2023 ("BSA"), which replaced the Indian Evidence Act, 1872, unequivocally brings electronic and digital

[7] Fed. Bureau of Investigation, Malicious Actors Manipulating Photos and Videos to Create Explicit Content and Sextortion Schemes, Public Service Announcement No. I-060523-PSA (June 5, 2023).
[8] Fed. Bureau of Investigation, Oversight of the FBI Cyber Division.

records under the ambit of evidence law. In particular, the BSA sections relating to electronic or digital records (sections 61-63) address their existence and admissibility.[9]

Section 61 explicitly provides that an electronic or digital record cannot be denied the quality of legal significance solely on the grounds that it exists in an electronic or digital form. Section 62 lays down the conditions for proving such a record, and section 63 defines their admissibility.[10] The legislative effort is, thus, a recognition of the reality that significant information can manifest and be preserved only in digital format. The BSA also makes it mandatory, for specific electronic records, to produce a certificate in the prescribed form which must include particulars about the device or source from which the record was derived and should attest to the hash value of the electronic or digital record.[11] The hash is valuable because it could assist in establishing whether the digital file produced later in time in court is the same as the digital file that was captured at the outset.

This statutory regime builds upon principles that were established by the Indian Supreme Court, prior to the enactment of the BSA, based upon the provisions of the Indian Evidence Act, 1872. In the case of *Anvar P.V. v. P.K. Basheer*, the Supreme Court had deemed the statutory requirements governing electronic evidence as a separate evidentiary regime.[12] This assertion was later clarified in the three-judge Bench judgment in *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, where it stated the significance of the certificate requisition, especially in the case of secondary electronic evidence, whilst distinguishing between the production of original electronic record versus submission in the output/copy produced in respect of the same.[13] It is therefore evident that the transition from section 65B of the former Act to section 63 of the BSA represents a significant continuity in our approach and a legislative streamlining.

Similarly, our procedural framework has seen increasing accommodation of digital modes of investigation. For instance, the Bharatiya Nagarik Suraksha Sanhita, 2023 ("BNSS") requires searches and seizures to be documented by means of audio-video recording by virtue of section 105.[14] This is an important procedural step as the manner in which devices or articles containing electronic information were discovered, seized and handled can impact the credibility of the evidence introduced at the trial.

3.2 Admissibility, Authenticity and Integrity

However, the existence of a statutory mechanism for admitting electronic records into evidence doesn't solve the challenge that deepfakes present. Admissibility and authenticity are two different, though related, issues. A recording may fulfil the procedure pertaining to its production and certification by the authorities but the contents within the said recorded materials could have been digitally manipulated to the core. While a certificate can vouch for the contents relating to how the record came into existence and from what source, it cannot, on its own, certify that every image, sound or utterance within such a record represents a real event. This becomes particularly pertinent when AI is used for altering the constituent components of the recorded materials.

Therefore, although the recognition of hash values and device-specific data in the BSA is of considerable help, it should not be conflated as a panacea to the synthetic data problem. A hash can attest to

[9] Bharatiya Sakshya Adhiniyam, §§ 61–63.
[10] *Id.* §§ 61–63.
[11] *Id.* § 63(4) & sched. (prescribing the certificate and requiring identification of the digital source and hash value).
[12] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.
[13] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
[14] Bharatiya Nagarik Suraksha Sanhita, 2023, § 105.

the integrity of a file at a certain time of its retrieval but not necessarily to the fact that the file was not generated or manipulated prior to its capture. Deepfakes, hence, take the examination from the stage of integrity of a digital file to the question of how and from what event the file originated.

3.3 Limitations of the Existing Framework

This legislative framework has laid a foundation for dealing with electronic evidence in India, but deepfakes highlight a critical gap. The legal frameworks for electronic evidence were primarily aimed at the acknowledgment of, and procedures for, production and verification of electronic records. Synthetic media adds a new level: content-level authenticity. A determination as to whether a digital record is technically sound cannot always be equated with a determination as to whether it truthfully depicts reality, and herein lies the crux of the evidentiary difficulties posed by deepfakes.

4 Deepfakes as Synthetic Evidence: Problems with Authenticity and Reliability

4.1 Authenticity of Synthetic Evidence

The foremost evidentiary challenge posed by deepfakes is that an electronic file may be accurate in form, while being falsified in its representation of events. Existing rules regarding electronic evidence predominantly centre on establishing the identity of an electronic record and how it was created and preserved. Deepfakes add a separate issue: whether the content itself correctly depicts an event as it unfolded. The importance of this distinction can best be illustrated by an unaltered recording that portrays a fabricated event.

Under the BSA, a compliant electronic record, meaning, it satisfies all relevant provisions pertaining to it, will be admitted before a court. But the admission of this electronic record to be a record that was actually created, does not signify its content's truthfulness. For example, a photographic, audio, or video record, when properly taken from an electronic device, and its contents' integrity is maintained once recovered/obtained, will in truth not convey any meaningful information about an event if its contents themselves are a falsehood.[15]

At present, there are two levels of authentication involved. The first is authentication relating to the integrity of the record: where the produced electronic file is indeed the file collected or retained from the device. The second authentication relates to the authenticity of the content in the record: is the person in an audio/video recording actually saying what the record purports the person to say, did the event take place at all and is the person who appears to be speaking/participant truly the person whose statement is reported. This second level of authentication becomes acutely challenging with deepfakes.

4.2 Metadata, Hash Values and Forensic Examination

While metadata, time-stamps and hash values serve vital functions in the examination of an electronic document, they should not be conclusive proofs of a substantively true record. A hash value confirms that an electronic file remains unchanged from the time its hash value was computed; it cannot provide proof that the file was not modified prior to the computation of the hash value. Correspondingly,

[15] Bharatiya Sakshya Adhiniyam, §§ 61–63.

metadata only confirms aspects like the date a file was created, edited, or sent; however, the metadata may also be incomplete, edited or deleted with ease.

Technical methods of preservation are thus just one level of an examination, rather than a complete test for truth. The hash-value and certificate provisions of the BSA only enhance the chain of custody of an electronic document but cannot, in and of themselves, provide substantive proof of a seemingly factual deepfake video.[16]

Thus, the relevance of expert witness testimony is now heightened more than ever in deepfake cases. Authentication tests require analysis of audio characteristics, visual inconsistencies of facial structure/movement, file compression parameters, incorrect lighting as well as frame-level inconsistencies, etc., and only specialized practitioners equipped with sophisticated software can identify them. A major practical issue in such tests is the rapid evolution of creation technology, posing a risk to the reliability of existing detection techniques that identify certain markers of fabrication.

Indian evidence law already accepts witness expertise on 'questions as to identity of handwriting or finger impressions' as science or specialized knowledge wherein a court must form an opinion.[17] Likewise, expert analysis will have a role in the trial of deepfake evidence as it can guide the court's opinion on authenticity. But just as with any other evidence, expert testimony does not command or replace judicial assessment; the trial court will have to evaluate the entire evidence while keeping in mind the specialized nature of such proof and the methodology and materials involved in the forensic examination.

4.3 The Liar's Dividend and Evidentiary Reliability

The challenge operates in reverse also. Given how commonplace convincing fabrication may become in the future, a party could possibly claim that an authentic electronic recording depicting inconvenient actions on his part is a forgery without substantial technical grounds. This has the unfortunate consequence of creating what has come to be called "the liar's dividend": The higher the belief society develops of truly deceiving falsified records becoming increasingly easy to produce and use effectively, the easier it is for a fraudulent individual to deny or dismiss any genuine evidence of his actions.[18]

This creates a dilemma in the criminal justice process: The court can neither accept a digitally manufactured recording purely based on an external, convincing appearance; nor can a seemingly credible piece of evidence be rejected simply by virtue of the fact that scientific technology allows for alteration. Blindly trusting digitally recorded evidence, believing it to be as valid as the original, and deeply distrusting it, believing it to be fake, would both represent extremes and would be equally detrimental for the search for an authentically produced digital record. Unfortunately, this is reflected in the existing framework of proof.

While there are procedures governing electronic evidence, some involving the requirement that evidence must be verified (such as the maintenance of integrity of the digital evidence recorded), they do not deal specifically with deepfake-authenticity, and do not set standards for a judge on when to request forensic proof, to which level the data should be scrutinised, and how conflicting analyses on a deepfake's origin should be treated in the court.

---

[16] *Id.* § 63(4) & sched.
[17] *Id.* § 39.
[18] Chesney & Citron, *supra* note 4, at 1785–86.

That's the problematic gap: When this gap arises in the context of a criminal procedure, where incorrect use of fabricated electronic evidence can cause a catastrophe just as well as authentic evidence can be unjustly excluded, the ideal solution therefore consists in establishing clear rules that allow for better identification of legitimate as against expertly manufactured synthetics in order to preserve a justice system able to handle and respond to challenges in the digital age.

5 Deepfakes and the Criminal Process: Investigation to Trial

5.1 Deepfakes at the Investigation Stage

The implications for the criminal process are far more far-reaching than a mere matter of admissibility of a particular recording. Synthetic media have the capacity to impact a criminal case at its earliest stages, with subsequent challenges and difficulties arising during the prosecution and trial. Indeed, a fabricated recording might be the genesis of an investigation, while an authentic recording might be thrown into doubt by the mere possibility of manipulation. Thus, rather than a singular test applied when the evidence has reached the court-room, the criminal process should build in protections at each stage.

The initial difficulty arises when a suspected deepfake comes to the attention of an investigator. A video clip, photograph, or audio recording might be received by a law enforcement officer from social media, messaging apps, or another digital source, without any reliable indicator of its authenticity. If such a recording is accepted as authentic without investigation and analysis, it has the potential to send an investigation down the wrong track, especially when it attributes the recording to a particular individual (who is then identified as the alleged offender). The opposite danger of rejecting a potentially fabricated recording without a full review, even when it might be relevant to the offence, is equally serious.

Hence, the correct approach of investigators ought to be to preserve the recording and investigate its origins before concluding its authenticity. Properly documented searches and seizures of electronic devices should also continue. The BNSS provisions which require that certain searches and seizures be recorded by way of audio-video electronic recording can be considered an example of how technology may be used to strengthen procedural safeguards.[19] Digital evidence's vulnerability to modification during copying, transmission, or file conversion necessitates that investigators maintain a clear record of when and where the item was obtained, from whom or which device, how it was stored, and by whom and when it was later accessed or handled. This forms a chain through which the evidence can subsequently be examined by the courts.

5.2 Forensic Verification and Evidentiary Challenges

When the authentic status of digital media becomes disputed, examination by forensic experts begins to become crucial. Detecting a deepfake is likely to require inspection of the underlying file itself, the context in which the original was recorded, and the method of its creation and dissemination. Investigators may be expected to compare the recording under suspicion with an original, analyse metadata, and identify inconsistencies or tell-tale marks.[20]

Also, the very use of fabricated media may be of some worry for the prosecution. For instance, where recording of the statement is of importance in terms of the conviction, it would only be a natural step

[19] Bharatiya Nagarik Suraksha Sanhita, § 105.
[20] Bharatiya Sakshya Adhiniyam, § 39.

for defence lawyers to attack the authenticity of the evidence and perhaps the prosecution would be expected to prove that the recording in question in actual fact accurately documents what it claims to record. The prosecution should not take advantage of apparent and natural realism and will find that the judge has to strike a balance between the admissibility, authenticity and probative value of the recorded media. We should not, just because synthetic media exists, abandon core principles out of ease.[21]

5.3 Impact on Fair Trial and Judicial Assessment

A fabricated recording has the potential to create guilt in the public's imagination through sight before genuine evidence of fact exists and this makes fabricated audio and video the gravest threat of them all. Once disseminated, even after its spurious origin has been discovered, significant damage to the accused's reputation may linger. In the context of the criminal trial itself, reliance on inaccurate synthetic material may serve to compromise proceedings on the grounds of fairness; the constitutional right to a fair trial guarantees not only protections from potentially unfair judicial procedures, but also protects genuine evidence from being dismissed based on unsupported claims of artificial construction.[22]

Five key issues arise from this analysis.

i. Firstly, that visual or auditory fidelity cannot reliably be considered an indicator of authenticity.
ii. Secondly, that the existing rules governing electronic evidence did not anticipate the rise of fabricated media and hence do not provide a framework specifically geared to verifying content authenticity.
iii. Thirdly, that while forensic techniques for detection are now developing apace, such analysis cannot be regarded as conclusive.
iv. Fourthly, that fabricated evidence is not only a danger in the sense of being admitted and having undue weight assigned to it, but that genuine evidence, especially if of a technical nature, may also wrongly be excluded as if it were artificial.
v. Fifthly, and finally, that combating deepfakes cannot merely be the province of the courts. Indeed, the investigators preparing cases, the forensic scientists who will analyse them, prosecutors who will guide them and defence attorneys who will test them will have to acquire a far greater capacity to deal with synthetic media and the challenges it poses to veracity.

The criminal process, therefore, cannot simply take technology's word for it. Instead, the investigation and adjudication of cases involving digital material necessitates a layered approach – involving careful preservation of original material, rigorous forensic analysis where necessary, expert opinions that articulate limitations as clearly as conclusions, judicial assessment of content that considers provenance over mere appearance, the seeking of corroborative evidence, and an increased awareness from all participants of the threat posed by synthetic evidence. Such a method is better suited to allowing courts to maintain openness to the truth contained in evidence that has been recorded by technology, without necessarily accepting such a recording at face value merely on account of its convincing appearance.

---

[21] *Id.*

[22] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473.

6 Enhancing India's Response: Legal, Forensic and Procedural Safeguards

6.1 Legal and Evidentiary Safeguards

The threat posed by deepfakes cannot be contained by simply adding new items to the cybercrimes list; the far more urgent need is to strengthen the means by which digital content is authenticated, inspected and presented before a court. What India needs is a holistic response consisting of corroborative protections, forensic capability, and institutional readiness. While the Bharatiya Sakshya Adhiniyam, 2023, already codifies evidence of electronically and digitally recorded records along with procedures for their admissibility (production and attestation),[23] deepfakes go beyond mere examination and require the court to ask if the recorded event and the content depicted actually occurred and is true in fact. Accordingly, specific principles of admissibility may be framed for deepfakes, especially when specific claims are made regarding artificial production of visual and audio evidence.

These principles aim not to indiscriminately bar deepfakes, but when authenticity is fairly put in issue and the recording is essential to the court's finding of facts, the court must have the power to demand some degree of forensic corroboration before admitting it as substantive evidence.

6.2 Forensic and Institutional Capacity

The need for specialized examination in deepfake cases cannot, therefore, be overstated. India requires adequate forensic labs and skilled personnel capable of analysing synthetic audio, still images, and video. Existing cyber-forensic facilities provide a base, but capacity should be expanded and made more accessible to various investigating agencies.[24]

Forensic reports should also, as much as possible, offer not only a simple "real" vs. "fake" verdict but also the underlying methodology and its limitations. Because synthetic content detection techniques evolve with generation techniques, judges must be able to assess the reliability of the methods employed in individual cases.

6.3 Preservation, Provenance and Stakeholder Training

Investigators should attempt to preserve original digital material whenever possible, in preference to relying solely on screen captures or forwarded versions. It is important to systematically document provenance, device of collection, relevant metadata, and subsequent handling of the digital content. The BSA provisions related to electronic evidence and hash values are helpful to confirm the integrity of preserved content but they should not imply that non-alteration after collection equates to original authenticity.[25]

All parties engaged in the criminal process – judges, police, prosecutors, and defence lawyers – need increased awareness of deepfake technology and digital forensics. While judges need not become technicians, a general understanding of how synthetic content is generated, and its detection, is valuable for judging expert testimony. Similarly, investigators and prosecutors should have a trained eye to identify suspicious digital evidence and not solely treat realistic-appearing audio or visual media as de facto proof. Defence lawyers can then use this training to raise proper challenges to the authenticity of evidence when there is real doubt.

---

[23] Bharatiya Sakshya Adhiniyam, §§ 61–63.

[24] Central Bureau of Investigation, National Cyber Forensic Laboratory, Government of India.

[25] Bharatiya Sakshya Adhiniyam, 2023, § 63 & sched.

A balanced response should safeguard the interests of victims while respecting the rights of the accused. Deepfakes can be used to promote sexual abuse, harassment, impersonation and fraud, but fake incriminatory evidence can similarly prejudice an innocent party. It is now also possible to dismiss genuine digital evidence on the ground of suspected falsity. The most balanced approach is therefore to focus on verification rather than assumption.

7 CONCLUSION

The impact of deepfakes on the relationship between technology and criminal justice can be profound. While electronic evidence is already an integral part of crime investigation and trial process, synthetic media has added a completely different dynamic to our dependency on the basic tenet that if an image or video looks genuine, it probably is an authentic representation of an actual incident. Therefore, the issue is not only that data has been manipulated, but that reality, as presented by the data, is fake. The present framework of evidence law in India, particularly under the Bharatiya Sakshya Adhiniyam, 2023, lays down some fundamentals regarding the admissibility and proving of electronic and digital evidence. However, this article aims to show that the standard requirements of the genuineness and integrity of digital evidence are not in and of themselves adequate enough to deal with the problem created by advanced synthetic material. A deepfake, while being sound, can be fake at the source. This creates an important difference between digital soundness and factual authenticity. The influence of the deepfakes affects several processes in the criminal trial, including the investigation, the scientific analysis of digital information, prosecution, the court's decision to judge the very authenticity and also the undue exclusion of genuine evidence out of fear that it might be synthesized. This is referred to as the liar's dividend, which will further reduce credibility. Hence, to address this problem there has to be an approach comprising reliable preservation measures, chains of custody, scientific expertise, expert opinion, judiciary, and corroborative proofs. Moreover there must be a focus on investing in infrastructure of cyber security, scientific experts, and well-trained investigators, prosecutors and judges. In essence deepfakes do not make electronic and digital evidence inadmissible; rather, they emphasize the need for proving. The criminal justice system in India now needs an approach by which it can clearly distinguish what appears real from what is factually authentic. The system must adapt, evolve, and embrace this. Thus the approach to digital evidence in India in the coming time should rely not on what is visibly "seen" and "heard" but on what can be effectively substantiated and proved in the case.

* * *