AI-GENERATED EVIDENCE AND DEEPFAKES IN INDIAN CRIMINAL TRIALS: EVIDENTIARY LAW, PROCEDURAL SAFEGUARDS AND JUDICIAL STANDARDS

Maanya Singh, Chandigarh University

Introduction

The rapid development of AI has put the law of evidence in a whole new arena, and the issue of AI-generated evidence and deepfakes is one that has caught the attention of the legal community. In the context of criminal trials in India, the truthfulness of evidence is of prime importance in delivering justice. The emergence of AI-generated evidence and deepfakes presents both opportunities and risks in the context of criminal trials in India.

For instance, AI can now be used to generate synthetic audio, video, or even documents that are extremely convincing. In the context of deepfakes, the reality can be distorted in such a way that it is extremely easy to deceive the court and all the parties involved in the criminal justice process.

In this article, I explore the legal and constitutional issues that AI-generated evidence and deepfakes are creating in the context of criminal trials in India. The article is titled "AI-Generated Evidence and Deepfakes in Indian Criminal Trials: Evidentiary Law, Procedural Safeguards, and Judicial Standards."

In this article, I have attempted to draw some valuable insights from the way in which these issues are being tackled in other countries and have also attempted to provide some valuable suggestions that can be implemented in the context of India.

Keywords: AI-generated evidence, Deepfakes, Bharatiya Sakshya Adhiniyam 2023, Fair trial, Digital evidence admissibility

What is AI-Generated Evidence and Deepfakes

AI-generated evidence refers to any form of proof in a legal proceeding that is created,

reconstructed, or significantly altered using artificial-intelligence tools[1]. In criminal trials, this may include synthetic text documents, audio recordings, video clips, images, or metadata generated by large language models, generative adversarial networks (GANs), or other AI architectures. Traditional evidence is captured from real-world events, whereas AI-generated material can be false, fabricated, manipulated and a direct physical counterpart. This raises a serious question about authenticity, reliability and the potential for fabrication, especially when such evidence is presented as conclusive proof of criminal conduct.

Deepfakes are a subset of AI-generated media[2] in which a person's likeness, voice, facial expressions, or gestures are digitally synthesised to make it appear they said or did something they never actually did. In the context of criminal-law, deepfakes can be used to create fake confession videos, staged sexual-abuse clips, counterfeit authentication footage or doctored audio of witness statements. The most dangerous part of deepfake is that they exactly mimic the original version and the chances that court and the judges may not be able to find the difference between the original and the mimicked one and as a result the defendant can come in trouble.

Article 21 and the right to a fair trial

Article 21 of the Indian Constitution guarantees the right to life and personal liberty, which the Supreme Court has expansively interpreted to include the right to a fair trial[3]. Article 21 is just not a procedural formality but it is a substantive guarantee that the criminal justice system must work with transparency, impartiality and adherence with due procedure establish by law. In case of AI-generated evidence and deepfakes, the trails should take place very seriously so that no evidences can get hampered, manipulated or fabricated in the name of digital evidence.

A fair trial under Article 21 should meet the criteria of authenticity, reliability, lawfully obtained[4], and the accused has been given opportunity to challenge every piece of inculpatory

[1] Deepfake Evidence and the Indian Criminal Justice System (2025) accessed 6 April 2026; AI-Generated Evidence in Indian Courts: Admissibility, Reliability, and the Chain of Custody Challenge (2025) Indian Journal of Integrated Research in Law vol V issue V.

[2] Vibha Rana, 'Criminal Law in the Age of Deepfakes: A Looming Evidentiary Crisis' (2025) Jus Corpus Law Journal accessed 6 April 2026; R Singh, 'Deepfake Evidence and Criminal Trials' (2025) Journal of Legal Research and Policy.

[3] Maneka Gandhi v Union of India AIR 1978 SC 597; AI-Generated Evidence in Indian Courts (n 1) 196–197 (linking unreliable AI evidence to breach of fair trial under Article 21).

[4] Zahira Habibulla H Sheikh v State of Gujarat (2004) 4 SCC 158; Deepfake Evidence and the Indian Criminal Justice System (n 1) (noting that admission of deepfake evidence without scrutiny undermines Article 21 guarantee of fair trial).

material. When AI-generated videos, audio or documents are introduced as "proof" of criminal conduct, the burden of verification shifts onto the accused or the court, often without clear statutory or technical standards. If courts fail to authenticate the proves and gives any wrong judgement then right to fair trial is undermined. One wrong judgment due to synthetic material can directly impinges on the accused's life and liberty.

When decision-makers rely on opaque AI tools whose logic is not disclosed or explainable, the accused's ability to scrutinise the basis of the prosecution's case is weakened. This opacity strikes at the core of fair-trial principles, because the right to confront and cross-examine evidence is central to Article-21. Courts have emphasised that the state must not place the accused in a position where they are "fighting in the dark." Thus, any normative framework for AI-generated evidence must be calibrated to safeguard the Article-21-guaranteed right to a fair trial, ensuring that technology serves justice rather than subverting it.

Article 14 and the risk of deepfake-based discrimination

Everyone stands equal before the law - so says Article 14 of the Constitution. But when fake videos or AI-made proof enter courtrooms as proves then fairness starts to shade. Not everyone faces the same scrutiny, some groups bear more suspicion than others. These digital fabrications might seem non dangerous and neutral but one single step can ruin everything. When that happens, justice stops feeling universal. Synthetic content can quietly reinforce old biases under a new mask. The outcome? A gap between what the Constitution promises and what reality delivers.

Older records shape how AI learns to handle proof[5], yet those records frequently carry long-standing societal slants - like heavier monitoring in some areas, less attention toward specific crimes, or speech norms tied to one culture. These flawed patterns seep into software applied within legal processes, nudging outcomes off balance. A system shaped by uneven information could see people from overlooked groups as more dangerous without good reason, especially when guessing future crime hotspots. Unclear words or actions from certain populations might get labelled suspicious too fast under such tools. Fake videos make matters worse, since they can twist someone's image to mock or single out entire communities. Courts might start seeing

[5] NAVIGATING DEEPFAKES IN INDIAN CRIMINAL LAW (2025) Indian Journal of Integrated Research in Law.

a person's background before seeing what actually happened.

Fake videos or audio might damage someone's standing in society. Though made up, they show people - often women, minorities, or rivals - in sexual, odd, or unlawful ways. Once seen in hearings or shared widely, these clips shape opinions about guilt or honesty, regardless of their truth. Even if disproven later, they stick, nudging judgments about a person's nature. Courts may lean on bias instead of law, especially when those biases are built into artificial intelligence tools. Fair treatment under the constitution fades, since results hinge less on facts more on deep-seated assumptions fed by machines.

Looking at legal principles, Article 14 demands fair, consistent, yet flexible ways governments gather proof and reach decisions. When tools powered by artificial intelligence or fabricated media harm specific communities more than others - lacking clear, balanced reasoning - it opens doors to claims of unfair treatment under that rule. To counter such risks, systems handling machine-made or altered digital content need strong checks; one example involves required reviews showing how these technologies affect different people. Openness about inner workings matters too, along with regular oversight done independently. Built-in fairness, not just efficiency, must shape each phase where automated aids are used inside court processes. Otherwise, trust in equal justice slips away despite technological progress.

Presumption of innocence and burden of proof in the age of synthetic evidence

Innocence stays with the accused unless proven otherwise - that's how criminal justice works. Prosecution must show guilt so clearly that no real doubt remains, at least in India. The person charged does not have to defend themselves; they start free of blame. Courts treat this idea as more than tradition - it lives within the Constitution too, tucked under fairness and life rights. Yet now, with fake videos and digital tricks spreading, trusting what seems like proof gets harder every day.

Picture something that looks real but isn't. Even when proven false afterward, a lifelike clip of someone appearing to commit a crime sticks in people's minds. Courts feel it too - eyes and ears often outweigh logic. Once such material enters a trial as undeniable proof, the person on trial ends up scrambling to show it's not true. Suddenly they carry the weight of disproving what shouldn't have been trusted so easily. That tilt in responsibility breaks the rule: guilt must rest solely on the shoulders of those making the accusation.

Most trial judges lack the background to grasp how AI-made videos or audio really work[6]. When rules inside criminal process laws do not spell out clear steps, people facing charges might struggle to challenge fake digital proof. Without required access to specialists or lab checks, computer-generated files could enter court unchecked. That reality chips away at the idea that someone is innocent until proven guilty, since defendants face high-tech barriers alone. Few safeguards mean flawed tech evidence risks distorting justice.

Still, doubt comes first when fake videos or audio enter court[7]. Because machines can now mimic reality, every piece of digital proof needs extra scrutiny. Only after clear verification should it even be considered real. Those offering the evidence must show how it was made, where it came from, otherwise it stays out. Defendants ought not have to prove something false; instead, those accusing must prove it true beyond normal checks. Without rules forcing this shift, old legal promises start to crumble under new tech pressures. Sooner or later, trust in fairness depends on these changes taking root.

The Indian Evidence Act and AI-Generated Evidence

India's rules for digital proof and private data come mainly from two laws: the 2000 IT Act and the 2023 DPDP Act. Though separate, they work together when tech handles personal details. Electronic files, online marks, and computer crimes fall under the older act. When it comes to info like fingerprints or movement trails[8], the newer law steps in. Since smart software feeds on vast pools of user data, both acts touch areas shaped by AI output. Authentication tools such as coded digital stamps - backed by Sections 3A and 10A - are recognized legally. Yet uncertainty remains around whether a piece of content came from a person or emerged from machine learning processes. Fake videos or made-up papers can look real, but the system lacks clear ways to tell their origin apart. A signature tied to a digital file might be checked through an IT Act certificate. Not proof of truth - only shows who sent it. What matters here isn't accuracy, but origin. The document could still mislead, even if the sender is confirmed.

[6] Deepfake Evidence and the Indian Criminal Justice System (n 1) (highlighting lack of technical capacity in trial courts and inadequacy of BSA for synthetic media)

[7] Anvar P V v P K Basheer (2014) 10 SCC 473; Arjun Panditrao Khotkar v Kailash Kushanrao Gorantyal (2020) 7 SCC 1 (on electronic evidence certification, now under Bharatiya Sakshya Adhiniyam 2023); Rana (n 2) (advocating prosecution must prove authenticity of synthetic evidence).

[8] Information Technology Act 2000, ss 3A, 10A; Digital Personal Data Protection Act 2023 (DPDP Act), ss 4–8 (lawful, fair, transparent processing of personal data including biometrics); 'Deepfake Evidence and the Indian Criminal Justice System: Challenges of Authenticity, Consent, and Admissibility in Law' (2025) 7(6) International Journal of Forensic Medicine and Research 3313 accessed 6 April 2026 (discussing gaps in distinguishing AI-generated vs human-origin content under IT Act certification).

Verification focuses on identity, never facts.

Those who are handling personal information have to do so legally, fairly, openly while also keeping strong safeguards and taking responsibility. When evidence comes from AI, police forces or companies relying on such tech now face these rules just the same

Finding its roots in fair handling, the raw information must follow set rules when used. Should data carry bias, errors, or come from illegal sources while shaping AI for courtroom proof, it might clash with the DPDP Act's boundaries. Still, the law mainly guards personal details and private rights - strength of trial evidence sits outside its reach.

Here's a quiet truth, the rules around data privacy miss what courts demand when it comes to proof made by artificial intelligence[9]. Instead of working alone, laws like the IT Act and the new data protection law should line up with older ones - such as how evidence is handled and how criminal cases move forward. Laws should be made in such a way that ensure privacy of individual and reduce the risk of data leaks and scams.

Information Technology Act, 2000 and the Data Protection Regime

India's rules for digital proof and private data come mainly from two laws: the 2000 IT Act and the 2023 DPDP Act. Though separate, they work together when tech handles personal details. Electronic files, online marks, and computer crimes fall under the older act. When it comes to info like fingerprints or movement trails, the newer law steps in. Since smart software feeds on vast pools of user data, both acts touch areas shaped by AI output. Authentication tools such as coded digital stamps - backed by Sections 3A and 10A - are recognized legally. Yet uncertainty remains around whether a piece of content came from a person or emerged from machine learning processes. Fake videos or made-up papers can look real, but the system lacks clear ways to tell their origin apart. A signature attached to any of the digital file only shows that who sent it but the verification of identity of the sender is not confirmed. The document can mislead and no one will be held liable for it due to the reason of identity proof. The document becomes completely void just because of a fake and unidentified signature.

[9] Bharatiya Sakshya Adhiniyam 2023 (BSA), s 63 (electronic records admissibility, formerly s 65B); DPDP Act 2023; Maneka Gandhi v Union of India AIR 1978 SC 597 (Articles 14 and 21 linkage to fair procedure); Rana (n 2) (advocating integration of provenance logs, training data disclosure, and biometric safeguards to align privacy with evidentiary fairness under Articles 14 and 21).

Due to advancement of AI tools companies are getting highly dependent upon such tech and as a result fraud, scam, misinformation is becoming really common these days. Police forces are also using AI tech for documentation, evidences digital stamp, signature etc. Those handling personal information have to do so legally, fairly, openly while also keeping strong safeguards and taking responsibility. Finding its roots in fair handling, the raw information must follow set rules when used[10].

In order to ensure data privacy both the IT Act and the new data protection law should work together and come up with laws and solution and tighten the steps for managing face scams, digital scams, data training will help to create a personal boundary for privacy law while still standing strong in court. Fairness gets sharper too, shaped by basic rights people hold under Articles 14 and 21.

AI in Criminal Investigations and Trials

Law enforcement bodies in India have already included AI tools in their practices. The Delhi Police has started using facial recognition technology to identify suspects during protests. The National Crime Records Bureau has shown inclination towards predictive policing systems. Forensic labs have used AI for handwriting and image analysis. While these tools prove to be advantageous in investigations, but their admissibility still remains unsettled in court. Use of technology in limited context has been permitted by Indian courts, such as, video conferencing testimony in the case of State of Maharashtra v. Dr. Praful Desai[11]. In some cases, courts have accepted CCTV footage as evidence, but only if it's been properly certified[12]. But there is still no precedent directly addressing AI-generated evidence.

Procedural Safeguards in Criminal Procedure

A system for handling criminal cases in India comes from the Code of Criminal Procedure, 1973. When fake videos or computer-made proof appear, parts of that code need closer attention. Because such tools can distort truth, rules around them require careful reading. Fairness during court hearings depends on how well those procedures hold up. Without strong

[10] DPDP Act 2023, ss 4, 7; NAVIGATING DEEPFAKES IN INDIAN CRIMINAL LAW (n 3) (biased or unlawfully sourced training data may breach DPDP fair processing but falls short of addressing core evidentiary strength under BSA).
[11] State of Maharashtra v. Dr. Praful Desai, (2003) 4 SCC 601.
[12] Ram Singh v. Col Ram Singh, 1985 Supp SCC 611.

checks, a person's right to equal treatment might weaken. So too could trust in legal decisions if false material slips through. How courts respond shapes whether justice stays reliable.

Right off, rules about sharing information need tightening. Prosecutors have to hand over key evidence to those charged, yet too often that means just paperwork, interview notes, or lab results. These days, when artificial intelligence helps produce proof, what gets shared should go further - code used, how systems were trained, model settings, even flaws or slants baked in. Missing these details leaves defendants unable to properly question digital outputs. Judges might start pushing updated guidelines, calling for tailored submissions whenever AI plays a role in building cases.

Now imagine questioning not a person but a machine. The law says anyone can challenge proof brought forward, yet that idea usually points to people talking in court. Once software shapes what counts as fact, the system itself takes centre stage instead. Judges might then demand specialists appear who can walk through how such programs work, where they stumble, even why mistakes happen. Only by doing so could those accused get close to checking strength and truth like they do when facing another human on the stand.

One way to handle new types of proof is by setting up firm tracking steps. Like how real objects move from crime scenes into courtrooms, images or videos made by artificial intelligence need their own clear path. Each time one of these files changes hands or gets altered, it should leave a mark - time recorded, who touched it, what changed. Outside experts might check them later, making sure they haven’t been twisted beyond truth. Whenever edits happen, those details must come out in open. Rules like these help keep justice steady when facts start living inside machines instead of folders.

Judicial attitudes towards digital evidence in recent Indian judgments

Lately, Indian judges have spent much time wrestling with digital proof - emails, online comments, stored data. Not once did those rulings tackle AI-created files or hyper-real video fakes head-on. Still, they reveal how legal minds sort through bits and bytes today. What we see now might quietly set the stage for handling computer-made lies in courtrooms tomorrow. Judged on their own terms, electronic proofs often pass legal tests if they meet what Sections 65A and 65B of the Evidence Act spell out - mirrored roughly by Section 63 and subsection 4 under the BSA - along with linked parts in the IT Act. Landmark rulings from the top court

stress one thing: digital files need correct paperwork backing them up. Without that stamp, questions about tampering tend to surface fast. Not every glitch means fraud, though. Judges have said getting caught in rule minutiae misses the point - truth matters more than rigid process. Sometimes, tight procedures do more harm than good, especially when someone might exploit loopholes unfairly. Digital data? Easy to change. Even easier to fake well enough to fool eyes. That reality pushes scrutiny deeper than before. Now doubts grow louder about how real any screen-based proof truly is. With artificial intelligence making fakes smoother each year, trust won't stay automatic much longer. Lately, certain High Courts pointed out how tech can fake what looks like real proof. Yet across India, there's still no unified legal stance on such made-up data. Notably, judges lately hesitate before trusting only digital files, particularly when they might be altered. Instead of taking them at face value, courts regularly pair electronic records with something else - say, someone who saw the event, lab findings, or paper trails. Expect this habit of double-checking to carry forward when dealing with AI-made or deepfake content, where backup from separate sources will probably matter just as much.

Conclusion

Even when fake videos look real, fairness in court still matters - especially in places like India. What stands clear is this: rights under Article 21 and Article 14 should block unfair treatment caused by misleading algorithms or manipulated media. With the development of latest technology like AI which consider itself really smart and fast in every term and it may be true to some extend but the law already exists. And as per law no one can be held guilty without their crime is proved by the procedure stablished by the court. Various laws already exist to deal with different situations. With the growth of new tech area, the already existing laws are not fully efficient in covering those field. Court procedures need to sharper tools as well, sharing evidence early, challenging machine-based findings, testing fakes with the help of specialists will help in keeping truth intact. Without them, false visuals might affect the judgments, tilt outcomes and harm the defendant. Truth needs support, not just tradition. Till this time strict rules are need to be implemented as soon as possible. When AI is used as evidence it should be clear in our head that from where the AI is collecting data, how it is functioning and if the ai makes mistakes then there should be someone who should be held accountable for it. AI should never break the promise done to citizens like equality, justice, fairness etc.