VOLUME 6 | ISSUE 2

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

DEEPFAKES AND DIGITAL EVIDENCE: A NEW TEST FOR INDIAN COURTS

- Vishnu Vardhan G & Mahizhnan C[1]

ABSTRACT

India is facing a major challenge with the advent of new technology known as deepfake technology. Deepfakes are hyper realistic audio and visual content created through Generative Adversarial Networks (GANs) and advanced Machine Learning algorithms. [2] The combination of these technologies has raised several concerns within the Indian Criminal Justice System, with respect to; electoral fraud, loss of reputation, and safety of victims, particularly those who have been attacked with non-consensual sexual deepfakes.[3] At this time, the Indian Evidence Act (IEA) of 1872 (which is more than 150 years old) was developed to establish the guidelines for dealing with such evidences in criminal proceedings.[4] The current provisions of Section 65B of the IEA (because they were informed by the needs of electronic crime investigations) are ineffective when dealing with electronic evidence created through technology such as deepfakes which mimic human voices and physical characteristics with forensic precision that is virtually undetectable. [5]In this article, the author seeks to demonstrate that, based on an analysis of current evidence law in India, a comprehensive framework for authenticating, evaluating, and admitting evidence potentially created through deepfakes into the criminal trial must be created. To do this, the author compares the proposed Federal Rule of Evidence 901(c) and the NO FAKES Act (NFA) in the United States, the European Union's AI Act (2024), and some of the emerging judicial decisions being issued by Indian Courts concerning this issue (specifically, the DELHI HIGH COURT injunctions issued in May-July of 2025), and argues that the best approach to introducing deepfakes into evidence in criminal proceedings, would be through the implementation of a hybrid authentication standard that combines traditional methods of authentication with forensic computer-analysis capabilities, and a

[1] Student at SASTRA Deemed to be University
[2]Ian Goodfellow et al., Generative Adversarial Nets, Advances in Neural Information Processing Systems (2014).
[3]Robert Chesney & Danielle Keats Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 Cal. L. Rev. 1753 (2019)
[4]Ratanlal & Dhirajlal, The Law of Evidence (LexisNexis, 27th ed.)
[5]Indian Evidence Act, 1872, 65B

means of shifting the burden of proof from the prosecution to the defendant[6]. Finally, the author proposes that specialized procedural guidelines for the introduction and use of deepfakes in Criminal Trials be developed and made widely available to the public.

Keywords: Deepfakes, evidence authentication, AI-altered media, criminal procedure, Indian Evidence Act, digital forensics, burden-shifting, deepfake detection, fair trial rights, comparative evidence law.

INTRODUCTION

The rapid pace of technological advancement in Artificial Intelligence has resulted in the development of synthetic media, also known as 'deepfakes,' which are capable of creating or changing video/audio content with a precision that was previously not possible. The core of any deepfake is built using a type of Machine Learning algorithm called a Generative Adversarial Network (GAN). GANs learn from existing data and create a new type of media that cannot be easily differentiated from original content. In India, where there is now a massive digital footprint with over 850million internet users, deepfakes have started to be used for political manipulation, harassment, bullying/defamation of individuals, and/or exploitation through sexual means.[7]

The laws in India concerning the Criminal Justice system are based on the Indian Evidence Act of 1872. This Act is based on concepts and principles that were conceived before internet technology became commonplace. Therefore, there are no coherent legal standards in place for evaluating synthetically augmented evidence. In addition to this, high courts across the country have started to intervene in a manner that reflects the urgent need to come up with standards for evaluating digital evidence. [8]An example of this is the John Doe injunction (Sec 64 of the Indian Evidence Act) established by way of a May 2025 order from the Delhi High Court against deepfake fraud perpetrated by Ankur Warikoo and July 2025 orders from the Delhi High Court against Meta and X to take down AI-generated obscene images.

However, these civil remedies mask a critical evidentiary vacuum where Indian courts having no reliable standard for determining whether an audio-visual exhibit offered as evidence in a criminal trial is authentic, altered, or entirely fabricated.

The Indian Evidence Act's primary mechanism for admitting electronic evidence — Section 65B

[6]Mirsky & Lee, *The Creation and Detection of Deepfakes*, 54 ACM Computing Surveys (2021)
[7]Europol Innovation Lab, Facing Reality? Law Enforcement and Deepfakes (2022)
[8]Telecom Regulatory Authority of India, Indian Telecom Services Performance Indicators (latest)

certificates — requires certification by a person occupying a responsible position in relation to the operation of the relevant electronic system.This provision was designed for computer-generated metadata (bank logs, server records, system timestamps) where reliability inheres in mechanical, non-interpretive processing. Deepfakes present an entirely different evidentiary problem: the alleged evidence is itself the artifact of generative AI, not a byproduct of routine system operations.Requiring a Section 65B certificate for deepfaked video evidence — which may be created by a bad actor specifically to deceive—does not address the fundamental question of whether the media depicts real events or is synthetic.

This paper advances three central arguments:

First, Indian evidence law requires doctrinal reformation to distinguish between authentication (establishing chain of custody and mechanical integrity) and authenticity verification (determining whether synthetic media is actual or fabricated).The current framework elides this distinction, creating risk that AI-altered evidence passes authentication yet corrupts the trial's truth-seeking function.

Second, a hybrid authentication standard combining traditional authentication, forensic AI analysis, and burden-shifting mechanisms offers a pragmatic path forward.Inspired by the U.S. Advisory Committee on Evidence Rules' proposed Rule 901(c) and adapted to Indian procedural contexts, this approach requires: (1) traditional authentication under Section 65A-65B; (2) if challenged, a preliminary showing by the opponent that the evidence could be AI-generated; (3) once credible challenge is made, the proponent must demonstrate authenticity by a preponderance of probabilities using forensic and contextual evidence; and (4) heightened corroboration requirements for convictions resting substantially on contested digital evidence.

Third, comprehensive procedural and institutional reforms — including specialized protocols for suspected deepfakes, court-linked digital forensic laboratories, and revised practice directions — must accompany doctrinal change.Evidence law alone cannot solve an institutional capacity problem.

The paper further addresses deepfake liability (Sections 66E, 66D, 67 of the Information Technology Act, 2000; Sections 111, 336, 353, 356 of the Bharatiya Nyaya Sanhita, 2023) and proposes a dedicated statutory framework for deepfake cyber-harassment crimes, informed by comparative

study of the EU AI Act and the U.S. NO FAKES Act.

THE INDIAN EVIDENCE ACT AND ITS INADEQUACY IN THE AGE OF DEEPFAKES

Sections 65A and 65B of The Indian Evidence Act, 1872 represent new developments introduced into the statute book as part of The Information Technology Act, 2000. These sections, therefore, bring Indian Law in line with modern developments concerning the use of electronic evidence.Under Section 65A, statements made using a computer will be deemed as being true unless the opposite can be established. This provision may apply to all electronically generated statements, as long as the computer was operational at the time of creating the evidence, and was routinely used for business purposes. Section 65B contains the requirement that electronic evidence must always have a formal certificate attached stating the type of device that was used to create the evidence, where the device can be found, who operated the device, the steps taken to ensure the evidence is accurate and reliable as well as the signature of an authorised person. In Anvar P.V. v. P.K. Basheer (2014)[9], The Supreme Court of India has ruled that evidence created on a computer will only be allowed if a strict compliance has been made with Section 65B(4). This was done in order to ensure that automated systems create reliable evidence that does not allow for any manipulation by a human.

Originally, the provisions were meant to allow for metadata (in the case of emails) generated by a system to be authenticated as being generated by a computer rather than providing proof of the factual accuracy of the record. On the issue of deepfakes, however, the AI-generated videos are created by computers and can contain purely imagined activities or events depicted in the videos; thus, someone with ill intent could generate a certificate from a provider that complies with section 65B, and produce that as acceptable evidence, even if that evidence is false. The Allahabad High Court in Satish Kumar Singhania v. State of Uttar Pradesh[10] found that failure to produce such a certificate would render any evidence inadmissible. To date, however, no court of appeal has ruled on whether a validly certified synthetic deepfake would be admissible or subject to heightened scrutiny.

This presents a unique challenge to the best evidence rule, which requires that, in most cases, the original document or object be produced. When it comes to digital files, "originals" and "copies" are

[9](2014) 10 SCC 473
[10]2019 SCC OnLine All 1604

both essentially the same, but it is impossible to obtain an actual original source document for a deepfake. The only way to determine if a deepfake is accurate is through forensic examination, metadata analysis, and/or expert testimony. Consequently, deepfakes completely undermine the presumptions under section 65A regarding witness identification and the element of chain of custody, as the actual act of generating a deepfake constitutes the basis for deceptive conduct, rather than altering a product after it has been created.

DOCTRINAL ANALYSIS: STANDARDS FOR AI-ALTERED DIGITAL EVIDENCE

The classical evidence doctrine defines authenticity as a characteristic that can be attributed to a piece of evidence. So, while physical evidence and documentation authenticate based on author/origin, Digital Evidence has traditionally authenticated with regard to where the file has come from and if that file is exactly the same as the file has not been manipulated from the time it was originally created. Therefore, Authenticity needs to be redefined due to the advent of the "deepfake" technology. A deepfaked video can be considered authentic as a digital file, however, because it represents events that actually did not take place, it can't be considered an authentic piece of evidence since it represents fabricated or fictitious events. Therefore, courts must differentiate between the Authenticity of form (the genuine file) and the Authenticity of content (the truthful depiction of the alleged event), since deepfake evidence uses the human cognitive biases against them and creates a sense of authenticity, in a way, past human defenses against their own perceptions. Therefore, courts need to maintain a heightened Epistemic standard that assumes that until verified with forensic AI analysis, all technically sound evidence is presumptively suspect.

A certification of Section 65B confirms that a piece of evidence has been created by a particular source device and has not been changed. In contrast, forensics-based AI software determines if the information in the digital evidence was artificially created through facial expressions, vocal differences, or improper data coding. A new verification framework is necessary that utilizes both original methods of verifying a digital signature with forensic-based AI detection and corroboration of facts based on context. The core methodology for this new multi-level system proposed by the author is: firstly, the proponent establishes Section 65B compliance (with forensics); secondly, the opponent challenges the original or newly produced evidence, triggering additional questioning of that evidence; and finally (aside from any possible challenges by the opponent), the proponent demonstrates the authenticity of the evidence through both AI-based analysis and corroboration of the evidence through judicial review of the evidence (if required) under Sections 104(a) and 132 of the Indian Evidence Act, 2013 (IEA). In this respect, Indian Law will evolve from being based on

"best evidence" to becoming increasingly reliant upon a verifiable method for supporting strongly the authenticity of synthetic forms of media.

COMPARATIVE JURISPRUDENCE: INTERNATIONAL APPROACHES

The framework for the authentication of electronic evidence in the USA is governed by Federal Rules of Evidence 901. Federal Rule of Evidence 901(b)(9)[11] deals with electronic records that were created by and retrieved from electronic systems. Federal Rule of Evidence 901 was initially designed for traditional digital records, such as emails and databases and does not address synthetic media. The Advisory Committee on Rules of Evidence has been working on this issue, in light of the emerging issues related to synthetic media and deepfakes, and proposed Federal Rule of Evidence 901(c), which specifically addresses "potentially fabricated or altered electronic evidence." This new rule establishes a burden-shifting procedure, whereby a Party challenging the authenticity of an electronic record must produce evidence to show that the item may have been created by generative artificial intelligence. If the Party producing the evidence meets this initial threshold, the proponent must prove under Federal Rule of Evidence 104(a) that the challenge is at least more likely than not true, as opposed to the former prima facie standard under Federal Rule of Evidence 901(a). The rationale behind this provision has been to treat deepfakes as "unmistakably authentic, although convincingly realistic fabrications" that would require additional safeguards, while at the same time eliminating nuisance or frivolous challenges. Federal Courts in the U.S. have begun to acknowledge that deepfake technology presents an issue with regard to the authentication of electronic evidence, specifically, deepfake technology presents a significant challenge with regard to the reliability of digital evidence in federal courts.

In a different context, the Artificial Intelligence Act (for the European Union) provides an ex ante regulation on deep fakes that consists of several articles, including:

1) Article 50 requires that deep fakes are disclosed in a machine-readable format, indicating they are AI-generated.
2) Some uses of deep fakes have been deemed "high-risk" by the European Union. These uses will require greater transparency than other uses.
3) Some uses of deep fakes will be categorically banned.
4) Monitoring of high-risk uses of deep fakes will need to take place after their initial release.

[11] https://www.law.cornell.edu/rules/fre/rule_901

As a result of these regulations, it is easy for users to verify the provenance of deep fake content.

In contrast to European law, India's recent judicial decisions on deep fakes as in Delhi's John Doe injunctions for Ankur Warikoo vsUndefinite person[12]are taking early steps toward recognizing the potential for deep fakes to cause significant harm to individuals, including through the violations of personality and privacy rights, and also creating obligations on platforms to remove them. These courts also have not yet addressed the issue of how deep fakes are to be treated as evidence in criminal trials.

NORMATIVE ANALYSIS: DUE PROCESS AND FAIR TRIAL RIGHTS

The Indian Constitution forbids compelled self-incrimination under Article 20(3) and guarantees life and personal liberty (Article 21). Fair trial rights have been interpreted by the Supreme Court to include these constitutional provisions and their requirement for conviction based solely on reliable and valid evidence. Deepfake evidence can violate both of these rights in two ways: First, deepfakes compromise the reliability of evidence because it is possible to create a deepfake video of someone (for example, making someone seem guilty) which may appear to be valid forensic evidence (due to it being perfectly made), thereby rendering traditional evidentiary protection ineffective. The second, and equally important, way that deepfakes threaten these rights is due to the lack of equal access to technology; prosecutors have the ability to fabricate evidence against a defendant, which creates a reversal of the presumption of innocence since the defendant must now prove the evidence's authenticity. Since the burden for proving guilt beyond a reasonable doubt assumes that the evidence is real, once the evidence's authenticity is in question, the burden must shift. Under the hybrid model proposed here, anytime a reasonably credible challenge to the authenticity of the evidence arises, it is up to the prosecution to affirmatively establish the authenticity of the evidence.

The changing landscape of evidence reflects the importance of judges assuming the primary responsibility of being the "gatekeepers" to evidence. In addition, because judges possess more sophisticated training and expertise than lay jurors, they are more qualified (under Section 104(a) and Section 132 of the Indian Evidence Act) to determine the authenticity of a deepfake and properly exclude any unreliable digital evidence. Therefore, given the implications of deepfake technology on how courts view evidence, the courts must develop a procedure for enhancing epistemic transparency by imposing stricter requirements on the corroboration of evidence, providing jurors with specific

[12]2025 SCC Online Del 3727

instructions about the potential risks associated with deepfakes, and limiting the use of digital evidence that is contested by the parties to use solely as supportive or detracting evidence. By doing so, the courts will maintain their constitutional mandate for due process while recognizing the epistemological uncertainties associated with synthetic media.

CRIMINAL LIABILITY: CREATORS, DISTRIBUTORS, AND PLATFORMS

The Indian legal system provides for several regulations on the use of deepfakes. Within that system, the Indian Penal Code of 1860 (IPC), the Information Technology Act of 2000 (IT Act), and the Bharatiya Nyaya Sanhita of 2023 create a comprehensive framework for regulating deepfake use.[13]

The IPC allows for regulation of deepfakes based on cheating, forgery and personation provisions (Sections 337-352), with maximum penalties for infringement being 7 years in prison. In addition to these provisions under the IPC, the IT Act prohibits impersonation over computers, violation of another person's right to privacy and distribution of indecent material online. Infringement of Sections 66D, 66E and 67 of the IT Act provides for 3 years of imprisonment and/or a fine up to ₹ 5 lakhs. The BNS incorporates new forms of liability for deepfakes that were not available under prior statutes by including provisions concerning misinformation (Section 111), organized crime (Section 319), personation (Section 336), and forgery (Section 356), which provide for general imprisonment terms of 3 to 5 years.

While the primary liability for producing harmful deep fakes lies with those who create the content, those who distribute this type of content may incur derivative liability if they knowingly distribute this information. One of the major doctrinal issues concerning deep fakes is determining whether someone who distributes deep fakes without knowledge of the contents of the deep fake is committing a criminal offence. As a general rule, intent or knowledge is required for a violation to occur; however, the BNS does extend liability to those who distribute deep fakes related to misinformation that creates a threat to public order under Section 353. Legislative reforms must be undertaken to make clear how much liability there is for each type of action regarding deep fakes. This will help to create a legal framework to differentiate between deep fake creators i.e.,who intentionally create them, deep fake distributors i.e., those who are aware that they are distributing

[13]Information Technology Act 2000

deep fakes, negligent distributors (who do not know), and those who use them innocently. Proportional Liability could be another way to divide liability equitably.

The psychological effects of NCII content that uses a deep fake are very gendered - the majority of victims are women. Still, the provisions outlined in sections 66E and 67 of the IT Act do not offer a full range of protections against creating or distributing deep fakes. Therefore, it is necessary for the Government to introduce specific legislation that prohibits the creation and distribution of sexual deep fake content without the consent of the individual depicted; that establishes strict punishments for violations (a minimum imprisonment of 5-7 years); enables extraterritorial jurisdiction to prosecute and punish offenders; and allows for civil recovery by victims. Furthermore, it will be important for Section 79 of the IT Act to transition from providing a blanket immunity to provide a qualified safe harbour by mandating that all deep fake content be detected using algorithms, moderated through a transparent process and removed from the platform within 36 hours of being reported, as highlighted by the Delhi High Court in its Meta and X decisions referenced above.

LEGISLATIVE REFORM: DESIGNING A DEEPFAKE OFFENSE REGIME

The European Union (EU) AI Act has proactively established an effective regulatory framework over the development and use of AI systems that can create deep fakes. The EU AI Act requires transparency by labeling AI-generated content with machine-readable labels. It also identifies deep fakes that qualify as high-risk and places these in a separate category for tighter compliance; restricts certain applications, including social scoring and surveillance; and provides for an ongoing monitoring and accountability mechanism after the deep fake is released to the public. Conversely, the proposed NO FAKES Act from the United States limits protection to the right of publicity of individual citizens by providing them with a private right of action when their likeness or voice is used inappropriately without their consent. The NO FAKES Act[14] establishes a range of damages between five thousand dollars to seven hundred and fifty thousand dollars per individual violation; ensures that companies that adhere to notification-and-remove processes are protected from liability; establishes a digital identification system to prevent future reuploading of material; and does not require any type of proactive review of uploaded content. The law in India does not specifically provide any one laws that prohibit Deepfakes or Synthetic Media; however, different sections of each of the Indian Penal Code (IPC), Information Technology Act (IT Act) and the BNS Act currently protect victims against deep fake abuse. The existing framework is broken down into

[14]https://www.congress.gov/bill/119th-congress/senate-bill/1367

disjointed sections that create uncertainty about how to prosecute offenders, thereby limiting victims' ability to receive appropriate remedies and creating a varied approach between prosecutions of offenders.

In order to eliminate this confusion, Indian Jurisprudence needs to clarify whether Deep fakes should be treated as a Crime in and of themselves, or whether they are criminal acts only if the intent behind the expression of Deep fake Media is to cause harm. A Clear definition of a crime that creates a Deep fake for the intent to defraud, defame, sexually exploit, impersonate, manipulate or disrupt Public Process will promote the necessity of intent when determining whether a person commits a Crime, while protecting the legitimacy of Deep fake creation for Artistry or Educational use.

Proposed statutory definitions of “Deepfake Cyber-Harassment” shall create an offence for the intentional creation or distribution of synthetic media purporting to represent an individual in a False Manner.

In order to maintain the rights of the creator, there will be protections for consent, parody and academic use, while requiring the prosecution to prove intent. Provisions similar to those found in existing legislation, such as the UK's Online Safety Bill and South Korea's Special Act, have been discussed and proposed within the Indian context to create a legal framework that will define deepfake cyber-harassment and create an explicit provision for addressing psychological or reputational injuries stemming from synthetic media.

PROCEDURAL AND INSTITUTIONAL REFORMS

The courts in India aren't standardized in their protocol for deepfake's authentication and evaluation. They usually, therefore, rely on the judge's discretion. To bridge this gap, a model Practice Direction regarding Deepfake Evidence could be introduced by either one of the High Courts or the Supreme Court of India. This would set out structured procedures for managing deepfake evidence in criminal litigation and obligate prosecutors to disclose the origin and chain of custody of all audio-visual evidence at a preliminary stage as well as require defendants, who are contesting the authenticity of audio-visual evidence, to disclose both the exhibit number and the reasons for contesting its authenticity (i.e. deepfake or edited). Furthermore, it would require the parties to designate experts to assist the tribunal (as per section 143 of the Indian Evidence Act) and expressly permit both parties to appoint forensic AI experts and to consult with court-appointed experts under Section 143. After

identifying experts, the tribunal would need to hold an evidentiary hearing before trial, either privately or publicly, to determine whether the subject audio-visual evidence is admissible based on the preponderance of evidence. In this type of hearing, the prosecution must establish that the audio-visual evidence meets the requirements of Section 65B and provide a valid analysis of its integrity. Conversely, the defendant must present evidence that challenges the evidence's authenticity and context (i.e. deepfake detection and challenge to the evidence's context). Once such evidence is challenged, authenticated evidence must be proven to a higher standard (i.e. the "clear and convincing" standard) before a conviction can be entered relying to a significant extent on audio-visual evidence. In addition, the statute requires independent evidence to support a conviction, as per Section 114.

Through the establishment of digital evidence integrity laboratories associated with high courts, a state can create a separate, neutral facility for the verification of digital evidence that uses an independent body to provide supporting expert testimony, training and research, funded in part by state or local grants and partially by user fees for those able to pay, but also including waivers for indigent defendants (in conjunction with partnerships with academic institutions offering forensic AI programs through IITs). Finally, establishing rules for corroboration will eliminate the use of unstably contested recordings as sole evidence, requiring that a non-recorded witness (e.g., eyewitness, physical, location or forensic evidence) corroborate their existence, thus excluding any derivative digital evidence derived from a single source as weak corroboration.

SYNTHESIS AND RECOMMENDATIONS

Under the Indian Evidence Act, Sections 65A and 65B note electronic evidence, including System Generated Metadata and Digital Evidence that are sufficiently authenticated, but do not apply to “Deepfakes,” or Digital Synthetic Media that are visually Indistinguishable from the Genuine Article in terms of Appearance of the Person in a Video. Certification is strictly limited to the Technical Integrity of the Files and does not authenticate that the Content depicts Real Events. Thus, this Doctrinal Shortcoming exposes Individuals to the possibility of Being Wrongly Convicted or Acquitted Based on Falsified Evidence, as well as jeopardizing the Integrity of the Court Process and Inverting the Presumption of Innocence.

To address this concern, proposed doctrinal reforms include redefining the Definition of Authenticity in order to Distinguish between the processes of Authenticating a Chain of Custody, and verifying the Content of a File, including a Hybrid Four Stage Standard, i.e.

(1) the Proponent must demonstrate Traditional Authentication of Digital Evidence in accordance with Section 65B;

(2) a Credible Challenge is raised by the Opponent;

(3) the Proponent must present a Preponderance of the Evidence in Support of Their Claim, which may require Forensic AI and Corroboration; and

(4) Judicial Gatekeeping is to be Excluded from the Jurors' Determinations. Furthermore, the Burden of Proof is to Shift to the Prosecution upon Challenge, requiring the Prosecutor to Provide Evidence to Establish the Prosecution's Case; and Independent Corroboration is required for any Conviction which is Largely Based Upon Challenged Digital Evidence.

Statutory reforms include the Creation of a single Deepfake Offence for Intentionally Creating or distributing Deepfakes to Defraud, Defame, Sexually Exploit or Impersonate, or Manipulate the Electoral Process. A New Cyber Harassment Offence would include an Aggravated Penalty for Sexual Deepfakes, be Extraterritorial in Nature, and more clearly define the criteria required for Safe Harbour Liability Limitation under Section 79/81. Procedurally, the Supreme Court or High Court would create Practice Directions requiring Courts to Conduct an Independent Investigation into Digital Elements of an Offence when the Offender's Intent was Established.

CONCLUSION

The advent of Deepfake technology has irrevocably changed the way evidence is assessed in criminal cases, revealing further limitations of The Indian Evidence Act, 1872 especially with regards to Sections 65A and 65B, which authenticate digital files as technical objects but do not confirm whether the content within these files portrays real-life occurrences. When a trial is compromised due to an inability to ascertain the authenticity of the underlying content there exists an increased potential for producing false convictions based on fabricated evidence and for producing false acquittals based on false challenges to the validity of the evidence; thereby reversing the order of presumption of innocence contained in Articles 20(3) and 21 of the Constitution.

The methodology of providing solutions involves: An identification of a doctrinal hybrid authentication standard distinguishing between both the technical integrity of the technical artifact (authentication under Sections 65A and 65B) and the authenticity of the evidence presented as content based (burden of proof shifting to the accused upon legitimate challenge and mandatory judicial review as per Sections 104(a), 132, and 143); The creation of a statutory provision for unified offences for creating deepfakes based on expressed intent as well as a similar statutory

provision for creating deepfake harassment; The development of procedure for the Supreme Court to implement formal Pre-trial Hearings in accordance with the directions of the Supreme Court to establish "Designated Expert(s)" and provide appropriate jury instructions regarding the potential dangers associated with deepfake evidence; The establishment of Digital Evidence Integrity Laboratories, which will develop the use of Forensic AI technology, and the establishment of judicial training regarding Forensic AI technology coherently integrated with the judicial process to enhance the forensic integrity of digital evidence.

The December 2025 draft A.I. draft rules published by the Centre, as well as the Injunctive orders issued by the Delhi High Court in 2025, concerning the cases of Ankur Warikoo, Sadhguru and Meta/X, are indicative of the current momentum in the judicial and legislative spheres in India. A pivotal moment to address this issue in India.