DEEPFAKE EVIDENCE AND THE CRISIS OF AUTHENTICITY UNDER THE BHARATIYA SAKSHYA ADHINIYAM, 2023: A COMPARATIVE STUDY WITH THE US FEDERAL RULES OF EVIDENCE AND EU AI ACT

***ANEEKA HIMAYAT**

ABSTRACT :

The Bharatiya Sakshya Adhiniyam, 2023 was set to act as a long overdue update to the Indian Evidence act, 1872. However, the Bharatiya Sakshya Adhiniyam, 2023, is coming out at a time when generative artificial intelligence raises questions about the reliability of audio visual recordings. Even though Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, talks about the certification process for electronic evidence previously recorded in Section 65B of the Indian Evidence Act, 1872, it only maintains its focus on verifying the source of digital evidence without properly authenticating the content.

This study revolves around three key research questions. The first question pertains to the admissibility of evidence that has been under the influence of deepfakes under the Bharatiya Sakshya Adhiniyam along with the conditions that govern it. The second question addresses which party bears the responsibility to prove or argue the synthetic nature of the digital evidence. The third question concerns itself with the necessary statutory, institutional and judicial reforms needed to bring the Bharatiya Sakshya Adhiniyam in line with the current advancements in generative artificial intelligence. To further understand these affairs, this paper executes a comparative study of three regulatory frameworks – United States adversarial system governed by Federal Rule of Evidence 901 and the Daubert Standard for expert testimonies, China's blockchain – based timestamping system. A system established by the Hangzhou Internet court. Lastly, the

*LLB, Rizvi Law Collage

requirements for transparency and labeling as enunciated in Article 50 of the Artificial Intelligence Act, 2024.

The current study examines the constitutional aspects of the already existing evidentiary gap, focusing on Article 14, Article 20(3) and Article 21. It analyzes how synthetic media can undermine fair trial protections, particularly identified as liar's dividend. This study concludes with a reform proposal that consists of five pillars – establishment of certified forensic resources, amendment in the Statute, mandatory training for judges, equal access to deepfake evaluations for individuals lacking financial resources and regulations for Intermediaries.

I. INTRODUCTION.

Consider the following scenario, that mirrors a growing trend of incidents being documented within the Indian Trail Courts : the defendant is being charged with homicide under Section 100 of the Bharatiya Nyaya Sanhita. The prosecution primary evidence in the case is a CCTV camera footage obtained from the petrol pump adjoining the crime scene, which allegedly shows the accused present at the crime scene at the time of the murder. This footage has been validated under what was previously Section 65B of the Indian Evidence Act, 1872, now referred to as Section 63 of the Bharatiya Sakshya Adhiniyam, 2023. The defense does not dispute the source of the CCTV footage. They also acknowledge the chain of custody of the CCTV footage. Instead, the defense submits that the individual in the video is not the accused, rather, they argue that the face of the accused has been digitally overlaid on the body of another individual through the use of artificial intelligence, specifically an application specializing in deepfake content, which is very easily available to the general public. The prosecution's witness, a senior police officer, claims that the CCTV footage was obtained from the hard disk without any modifications. The witness lacks the knowledge and expertise to ascertain whether the contents of the hard disk were ever authentic. To support the claims of the defense, the defense presents an expert who elucidates, using complex terms related to latent space and Generative Adversarial Networks (GANs) , why she believes the footage is fabricated.

This situation has shifted from being completely hypothetical. A deepfake video of the actress - Rashmika Mandanna gained significant traction on social media in November, 2023. This led the Ministry of Electronics and Information Technology[1] to issue an emergency advisory. Subsequently, deepfake videos of various high-profile individuals including politicians such as the Prime Minister were posted just before the general elections. The Delhi High Court addressed this issue in the case of Chaitanya Rohilla v. Union of India, where the resolution is still pending[2]. The Indian Judicial System has started to recognize this as a challenge, a challenge to which they don't have the necessary tools to address adequately.

Deepfakes emerge from a type of machine learning methods that until very recently were considered peripheral in the field of computer science. There are various types of deepfakes but the variant that receives the most attention employs Generative Adversarial Networks (GAN), a framework that Ian Goodfellow and his team unveiled in 2014[3].

A Generative Adversarial Networks (GAN), involves the working of two neural networks working against each other : one network, the generator, creates artificial outputs while the other, the discriminator attempts to differentiate the generators fake from genuine samples. After various revisions, the generator becomes skilled enough to create outputs that the discriminator and the human observer can no longer tell apart from real images. More advanced diffusion models like those used in systems such as OpenAI's Sora and Stable Diffusion generate images by refining random noise into clear pictures, and they have exceeded GANs in terms of photorealism[4]. In addition to photorealism, voice cloning technologies can mimic a person's vocal range and speech patterns with the help of a short reference of a few seconds.

---

[1] Ministry of Electronics & Information Technology, Govt. of India, Advisory to Intermediaries and Platforms (Nov. 7, 2023) [hereinafter MeitY Nov. 2023 Advisory], available at https://www.meity.gov.in (last visited May 12, 2026); see also Soumyarendra Barik, *After Rashmika Mandanna deepfake video goes viral, government issues advisory to social media platforms*, Indian Express (Nov. 7, 2023).
[2] Chaitanya Rohilla v. Union of India, W.P.(C) 15596 of 2023 (Del. H.C.) (pending); see also Rajat Sharma v. Union of India, W.P.(C) 6859 of 2024 (Del. H.C.) (pending) (sought regulation of deepfakes and intermediary obligations).

[3] Ian J. Goodfellow et al., *Generative Adversarial Nets*, in 27 Advances in Neural Information Processing Systems 2672, 2672—73 (Z. Ghahramani et al. eds., 2014).
[4] Jonathan Ho, Ajay Jain & Pieter Abbeel, *Denoising Diffusion Probabilistic Models*, in 33 Advances in Neural Information Processing Systems 6840 (H. Larochelle et al. eds., 2020); for the consumer-facing manifestations, see Robin Rombach et al., *High-Resolution Image Synthesis with Latent Diffusion Models*, Proc. IEEE/CVF Conf. on Computer Vision & Pattern Recognition 10684 (2022).

The significance of these technologies in the legal field goes beyond their ability to fraud the masses. They have disrupted the link between what we see and what the reality of the situation is. For over one hundred years, the Indian Evidence laws have relied on the principle of presumed authenticity. The principle of presumed authenticity means that any photograph, video or recording created correctly can be considered an accurate depiction of the subject. Nevertheless, this assumption can no longer be trusted. As warned by Citron and Chesney in their influential article, deepfakes inaugurate an era in which *"seeing is no longer believing"* and in which courts must learn to live with the corrosive doubt that any video may have been manufactured[5].

The Bharatiya Sakshya Adhiniyam, 2023[6] came into effect on 1st July, 2023 along with its partner legislatures - The Bharatiya Nyaya Sanhita, 2023 and The Bharatiya Nagarik Suraksha Sanhita, 2023. These acts presented the Parliament with an opportunity to tackle these issues. Unfortunately, the Parliament missed this opportunity. Even though the Adhiniyam broadens the scope of the term "Document" to cover both electronic and digital records and modifies the certification requirement from the previous Section 65B to Section 63, it fails to address emergence of synthetic media. There are absolutely no regulations related to artificially generated media or content. It does not mandate the disclosure of deepfakes. In addition, it also does not specify who is responsible for verifying the disputed digital evidence. The statute lacks any criteria for courts to assess conflicting forensic claims related to synthetic origins[7]. In compendium, the Bharatiya Sakshya Adhiniyam, 2023 reflects the digital landscape of the early 2010's, ignoring the boom of artificial intelligence.

This study is based on three key research questions. The first question being – Whether deepfake evidence can be accepted under the BSA, 2023 and if it came be accepted then what conditions apply. The second question focuses on which party is responsible for countering the synthetic nature of the evidence : the one presenting the evidence or the one contesting it. Lastly, the third

[5] Danielle Keats Citron & Robert Chesney, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, 107 Cal. L. Rev. 1753, 1758 (2019).
[6] Bharatiya Sakshya Adhiniyam, 2023, No. 47, Acts of Parliament, 2023 (India) [hereinafter BSA]. The BSA, along with the Bharatiya Nyaya Sanhita, 2023, and the Bharatiya Nagarik Suraksha Sanhita, 2023, came into force on July 1, 2024, vide Notification S.O. 850(E) (Feb. 23, 2024).

[7] BSA, *supra* note 6, § 63(4) (certificate requirement for electronic records).

question examines what changes in the procedure and law are necessary to update the Indian Evidence Laws to reflect the current state of artificial intelligence.

To answer these questions, this study focuses on the experiences of three different regions. The United Staes is dealing with evidence relating to deepfake via Federal Rule of Evidence 901 (which addresses authentication), Rule 702 (regarding expert testimony according to the Daubert Standard), and a complex array of various state laws. On the other hand, the European Union has introduced a labelling requirement for creators of synthetic content through article 50 and the AI Act, 2024 representing a structural change unlike any initiative from the United States or India[8]. Lasty, China has combined its 2022 Deep Synthesis Regulations with blockchain technology for time-stamping, an innovative method established by Hangzhou Internet Court[9]. Each of these frameworks provide insights for India while also having their respective limitations.

In short, the argument suggests that the Bharatiya Sakshya Adhiniyam, 2023 even when read with the Information Technology Act, 2000 along with the recent guidelines from the Ministry on Electronics and Information Technology lacks the necessary structure to manage evidence emerging from deepfake content. The certification required under Section 63(4) can confirm the source of a digital file but cannot ensure that the content itself is reliable. Section 39, which replaces the earlier Section 45 of the Indian Evidence Act allows for opinion evidence on technical matters. At present, India has no recognized deepfake forensic resources to provide authoritative opinions that would be significant in the courts of law. Article 21 of the Indian Constitution ensures a fair trial. It is unlikely to endorse convictions based on challenging synthetic media. Solutions to this must be legislative, institutional and judicial. This paper concludes with a suggestive framework that includes a new clause in the Bharatiya Sakshya Adhiniyam, 2023 – a requirement for labeling as per the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules of 2021, recognized forensic labs from the Indian Computer Emergency Response Team, and essential training for judges through the National Judicial Academy.

[8] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), art. 50, 2024 O.J. (L 1689) 1 [hereinafter EU AI Act].
[9] Provisions on the Administration of Deep Synthesis Internet Information Services (promulgated by Cyberspace Admin. of China, Ministry of Indus. & Info. Tech. & Ministry of Pub. Sec., Nov. 25, 2022, effective Jan. 10, 2023) (China), translated in DigiChina, Stanford University Cyber Policy Center, https://digichina.stanford.edu (last visited May 12, 2026).

II. BACKGROUND: THE EVIDENTIARY ECOSYSTEM IN INDIA

A. Historical evolution of Digital Evidence laws :

The story of digital evidence in India appears at first glance, to be a tale of gradual growth. The Indian Evidence Act, 1872 was modified following the introduction of the Information Technology Act in the year 2000 to include electronic records[10]. Now the Bharatiya Sakshya Adhiniyam, 2023 has slightly broadened and solidified those rules. Beneath that surface, however, lies a more troubled doctrinal history.

Section 65B of the Indian Evidence Act, read with the Information Technology Act 2000 established a unique framework for handling electronic evidence. Items such as computer generated prints, photographs, videos, emails or CCTV footage stored on a hard drive could only be admissible in court and be considered valid if it is accompanied by a certificate from someone in a *"responsible position in relation to the operation of the relevant device.[11]"* Even though the language of this provision was clear, implementing this section proved to be a challenge. For more than a decade and a half, Indian courts grappled with key issues including whether the certificate was essential or optional, if it could be submitted during an appeal, whether secondary evidence could substitute it and if the requirement could be waived when the party presenting the evidence did not have control over the device.

In the case of Anvar P.V. vs P.K. Basheer[12], a three Judge Bench of the Supreme Court determined that the existence of a certificate was essential and that the previous ruling in the state (NCT of Delhi) vs Navjot Sandhu[13], which allowed for the use of secondary evidence of electronic records without a certificate, was incorrectly made. Anvar P.V. effectively established, at least in principle that adherence to Section 65B(4) regarding electronic evidence was imperative. Be it as it may, the later ruling in Shafhi Mohammed vs State of Himachal Pradesh[14] cast uncertainty on this interpretation by stating that a certificate was not needed if the party presenting the evidence did

[10] Information Technology Act, 2000, § 92 and the Second Schedule (inserting §§ 65A and 65B into the Indian Evidence Act, 1872).
[11] Indian Evidence Act, 1872, § 65B(4), No. 1, Acts of Parliament, 1872 (India).
[12] Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, 485—86 (India) (Kurian Joseph, J., for the three-Judge Bench).
[13] State (NCT of Delhi) v. Navjot Sandhu, (2005) 11 SCC 600 (India), held that secondary evidence of electronic records could be tendered without a § 65B certificate; the decision was held per incuriam in *Anvar P.V.*, *supra* note 12.
[14] Shafhi Mohammad v. State of Himachal Pradesh, (2018) 2 SCC 801 (India).

not have control over the device. This created an unusual exception not grounded in the actual wording of the statute. Ultimately, in Arjun Panditrao Khotkar vs Kailash Kushanrao Gorantyal[15], a three Judge Bench reaffirmed the findings in Anvar P.V. vs P.K. Basheer and invalidated the Shafhi Moahmmad decision. Justice Nariman, on behalf of Court, characterized Section 65B as "a complete code in itself" and asserted that obtaining the certificate was *"a condition precedent to the admissibility of evidence by way of electronic record"*[16].

A discernible trend has emerged. Indian judiciary systems have regarded electronic records as generally valid, provided that the necessary certification procedures have been followed. The certificate acts like a key to the evidence – present it and the document is accepted. Failing to present the certificate leads to the evidence getting rejected. The essential nature of the evidence that is, its contents rather than its source was primarily left for the trial proceedings to assess. This approach proved effective in an era where the main risk of digital evidence was manipulation through editing – altering photographs, merging videos or modifying text messages. Nonetheless, this method is now insufficient in a time when an entire image or recording can be generated by a use of a simple prompt.

B. The Bharatiya Sakshya Adhiniyam, 2023 : What changed and What did not.

the Bharatiya Sakshya Adhiniyam, 2023, had been introduced to the parliament as an update to the Indian Evidence Act from the colonial period. When considering its structure, the new laws closely resemble the original. Numerous sections have merely been renumbered. The Section concerning the certificate of the electronic records, which used to be Section 65B is not designated as Section 63. In terms of admissibility in court, Section 61 places electronic and digital records on equal grounds with documentary evidence, while Section 39 which corresponds to the previous Section 45 allows for expert testimony on technical issues[17].

There are two notable alterations in the Bharatiya Sakshya Adhiniyam, 2023. Initially the term "document" has been explicitly expanded to encompass electronic and digital records, which

[15] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 (India).
[16] *Id.* at 27—28 (para 32), per Nariman, J.
[17] BSA, *supra* note 6, §§ 61, 63 & 39.

include communications saved in semiconductor memory or any other electronic format[18]. Secondly, Section 63(4)(c) now clearly mandates that the certificate must be signed not only by the individual using the device but also by an expert. This may indicate an understanding that solely administrative certification may not be adequate[19].

Unlike source authentication, the Bharatiya Sakshya Adhiniyam, 2023 lacks any rules for the verification of the authenticity of the content. There is also no presumption against evidence produced with the help of artificial intelligence, nor is there a specific process for addressing media claimed to have a synthetic origin. The individual presenting the digital evidence is not mandated to indicate if the evidence has gone through generative model or if it is a result of such model. In addition to this, there are no requirements for any pre – trial examination of the evidence. It appears that the authors of the Bharatiya Sakshya Adhiniyam, 2023 have focused on the classic forms of forgery, particularly those involving edits and have missed the chance to consider scenarios where a video may lack originality altogether. This gap is the primary issue discussed in this paper[20].

C. How deepfakes attack each pillar of Indian evidentiary standards.

Three pillars of contemporary digital evidence doctrine in India are particularly vulnerable to deepfakes.

The Section 63 certificate, whether in its current version or in a previous iteration, confirms that the data extraction process maintains integrity – specifically, that the bits and bytes shown to the court are indeed the same ones that were originally on the device. It neither confirms nor can it validate the connection between those bits and bytes and the actual events they are intended to represent. A flawlessly created deepfake stored within a CCTV system will meet the certificate criteria just as readily as an authentic recording. While the certificate ensures the integrity of the data's chain of custody, it does not address the veracity of the data itself.

[18] *Id.* § 2(1)(d) read with *id.* § 57.
[19] *Id.* § 63(4)(c) (requiring a certificate signed both by the person in charge of the computer and by an expert).
[20] Karnika Seth, *Computers, Internet and New Technology Laws* 412 (2d ed. 2019); for a recent comment see Ananya Bajpai, *AI-Generated Evidence in Indian Courts: Admissibility and Legal Challenges*, Lawjurist (July 2025) (on file with author).

The second pillar focuses on the chain of custody. In the physical world there was only the tangible evidence when it came to the chain of custody. For instance, a knife needed to be taken into possession, sealed and presented. In contrast, in the digital world it depends on the trustworthiness of cryptographic hashes and related metadata. A deepfake can be inserted anywhere within this chain – during the recording phase by an attacker who gained control of the device, during the extraction phase by an officer who replaces the original life with a synthetic version or at the submission stage by a party involved in litigation. The Bharatiya Sakshya Adhiniyam, 2023 does not stipulate that any of these moments must be supported by cryptographic verification. Notably, there is no obligation to obtain a forensic hash at the time of collection, a significant oversight considering that the methods for generating such hashes have been established for decades and are regularly utilized by advanced forensic agencies in other regions.

The third pillar receives less attention. It is known as the liar's dividend. This term was introduced by Citron and Chesney to capture a troubling second – order effect of the deepfake phenomenon. When it becomes common knowledge, that synthetic media is possible, any authentic media can be dismissed as fake[21]. A defendant, even when their actions are recorded on CCTV cameras, might succeed in creating reasonable doubt in a courtroom simply by suggesting the existence of manipulated content. These issues affect both – the delivery of justice, leading to instances of unjust acquittals along with wrongful convictions. The Bharatiya Sakshya Adhiniyam, 2023, by lacking a clear framework for assessing claims of synthetic origins, exacerbates the liar's dividend instead of limiting it.

III. COMPARATIVE ANALYSIS

A. United States: FRE 901 and the Daubert Standard

The American method of establishing authentication has a rich history. According to the Federal Rule of Evidence 901 (a), the party presenting the evidence must *"produce evidence sufficient to support a finding that the item is what the proponent claims it is"*[22]. This requirement is intentionally minimal. The issue of authentication resolves around conditional relevance, leaving

[21] Citron & Chesney, *supra* note 5, at 1758—60. The phrase "liar's dividend", coined at p. 1785, captures the corrosive evidentiary effect of mere knowledge of deepfake technology.
[22] Fed. R. Evid. 901(a).

it to the judge to decide if a reasonable juror could view the evidence as what it claims to be. Some instances of valid authentication are detailed in Rule 901 (b), which includes witness testimony, distinctive features and expert comparisons[23]. While Rule 902 outlines self – authenticating documents, such as certified data copies from electronic devices, a category that was expanded with the 2017 amendments.

In situations where authentication is disputed, expert testimony comes into play under Rule 702[24] and the Daubert Standard set forth by the Supreme Court in Daubert vs Merrell Dow Pharmaceuticals Inc[25]. According to Daubert, it is the trial Judges's role to act as a "gatekeeper" and assess if the expert's reasoning employs a methodology that can be tested, has undergone peer review, displays a known error rate and is widely accepted within the relevant scientific community[26]. Forensic detection of deepfakes, leveraging convolutional neutral networks designed to spot anomalies in generative outputs, is still in the early stages of development. There is considerable variation in error rates among various methodologies and certain published detection tools have demonstrated ineffectiveness when applies to deepfakes generated by unfamiliar models[27]. As a result, U.S Courts have approached this issue with caution. In the initial cases where evidence of deepfake detection was presented, motions in limine frequently led to exclusion based on Daubert criteria.

In addition to the progress made in the judicial system, state legislatures have taken assertive steps. Texas Senate Bill 751 (2019) makes it illegal to produce and distribute election related deepfakes within thirty days of an election[28]. Similarly, the California's Assembly Bill 730 (2019) puts similar limitations in place, while the AB 602 (2019) established a civil cause of action for

[23] Fed. R. Evid. 901(b)(1)—(10) (enumerating, *inter alia*, testimony of a witness with knowledge, distinctive characteristics, and comparison by an expert witness or trier of fact).
[24] Fed. R. Evid. 702 (Testimony by Expert Witnesses), as amended Dec. 1, 2023.
[25] Daubert v. Merrell Dow Pharms., Inc., 509 U.S. 579, 592—95 (1993). The Daubert factors were extended to non-scientific expert testimony in Kumho Tire Co. v. Carmichael, 526 U.S. 137 (1999).
[26] *Daubert*, 509 U.S. at 597 (Blackmun, J., for the Court).
[27] Luisa Verdoliva, *Media Forensics and DeepFakes: An Overview*, 14 IEEE J. Selected Topics Signal Processing 910, 925 (2020) (noting that detectors trained on one GAN family generalise poorly to outputs of unseen architectures); *see also* Riccardo Corvi et al., *On the Detection of Synthetic Images Generated by Diffusion Models*, Proc. IEEE Int'l Conf. on Acoustics, Speech & Signal Processing (2023).
[28] S.B. 751, 86th Leg., Reg. Sess. (Tex. 2019) (codified at Tex. Elec. Code Ann. § 255.004(d)).

deepfake pornography distributed without consent[29]. In other states, including New York and Virginia, have passed comparable laws. Although these regulations primarily focus on the production of deepfakes rather than their use as evidence, they are beginning to introduced key terminology – such as "materially deceptive content", "reasonable observer' and "malicious intent", that could eventually influence legal provisions for evidence.

The effectiveness of American methods stems from its adversarial structure – both parties present their experts, the judge oversees the process, and the jury reaches a verdict. However, a significant disadvantage is its reliance on equal access to expert resources. Often, a well-resourced plaintiff can hire three experts in the deepfake forensics field whereas a cash constrained defendant may only be able to afford one. Such imbalance can be somewhat controlled in commercial cases but is a major hurdle in criminal cases. The judge led system, which is unique to India and allows the court to seek expert opinion under Section 39 of the Bharatiya Sakshya Adhiniyam, 2023, has unique benefits. India lacks the robust network of competing private forensic services essential for providing the America system with its (albeit uneven) dynamism.

B. European Union: Artificial Intelligence Act Transparency Obligations

The European Union (EU) adopted a fundamentally different strategy. Instead of waiting for synthetic content to be confronted during evidentiary admission phase, the EU aims to identity synthetic content right from its creation. Article 50 of Regulations (EU) 2024/1689, the Artificial Intelligence Act, came into effect in August in the year 2024. It established obligations for suppliers of generative artificial intelligence systems to ensure that their outputs are *"marked in a machine – readable format and identifiable as artificially generated or altered"*[30]. Those who deploy such systems and create or modify content that qualifies as a "deepfake" are required to disclose information. There are limited exceptions for uses related to art, satire and law enforcement[31].

[29] A.B. 730, 2019—20 Reg. Sess. (Cal. 2019); A.B. 602, 2019—20 Reg. Sess. (Cal. 2019) (codified at Cal. Civ. Code § 1708.86).
[30] EU AI Act, *supra* note 8, art. 50(2).
[31] *Id*. art. 50(4); the definition of "deep fake" appears in art. 3(60).

The requirement for labeling fulfils two functions that are missing in the framework of the United States and India. It shifts the responsibility for disclosure from the challenger to the content producer. It also establishes an audit trail, at least theoretically – through which courts can ascertain if a specific media item was created by a compliant system. The implementation methods involve cryptographic watermarking and metadata signatures that adhere to the Coalition for Content Provenance and Authenticity (C2PA) standard[32]. In the future, hardware attested provenance documented at the moment of capture.

The Artificial Intelligence Act categorizes specific applications such as biometric identification and predictive policing, as "high risk", thereby needing further conformity assessment[33]. The Act does not explicitly govern the acceptance of artificially generated content proofs in national courts, where admissibility still falls under the procedural laws of each member state – Recital 132 suggests that labeling requirements will aid in evaluating evidence[34]. In addition to this, Article 22 of the General Data Protection Regulation, which affords data subjects the rights to not face decisions based exclusively on automated processing, could influence how police or prosecutors employs algorithmic methods in analyzing evidence[35].

The European Union model is attractive, by focusing on regulating creators instead of just addressing forgers it avoids certain types of legal disputed related to evidence. This model does have its constraints. Non-European Union developer's adherence is largely optional; watermarks can easily be removed through basic post – processing and the act does not extend its authority to open source models that are trained and distributed beyond the Union. For India, which relies heavily on generative artificial intelligence from providers in the United States and China, the European Union method should be seen as a partial remedy rather than a comprehensive solution.

C. China: Blockchain Timestamping as Evidence Authentication

[32] Coalition for Content Provenance and Authenticity, *C2PA Specifications v2.1* (2024), https://c2pa.org/specifications (last visited May 12, 2026).
[33] EU AI Act, *supra* note 8, Annex III (high-risk AI systems, including § 6 biometric identification and § 6(d) law enforcement use).
[34] *Id.* Recital 132.
[35] Regulation 2016/679, art. 22, 2016 O.J. (L 119) 1 (EU) (General Data Protection Regulation).

Among the three countries, China has showcased the most extensive reaction to synthetic media. In November of 2022, the Cyberspace Administration of China along with the Ministry of Industry and Information Technology and the Ministry of Public Security implemented the Provisions on the Administration of Deep Synthesis Internet Information Services, which became effective in January 2023. These regulations mandate the providers of deep synthesis services visibly label any artificially generated material and maintain logs for a minimum of six months[36]. In July of 2023, the Interim Measures for the Management of Generative Artificial Intelligence Services broadened these requirements to encompass all generative artificial intelligence available to the public in China[37].

The innovation in evidence is taking place within the courtroom setting. Since its establishment in 2017, the Hangzhou Internet Court has recognized digital evidence that is stamped with blockchain as valid in various intellectual property and contract disputes. The reasoning behind this is that a cryptographic hash logged on a secure distributed ledger at the moment of an alleged occurrence provides greater reliability than a narrative of chain of custody delivered by witnesses. This approach received support from the Supreme People's Court in its 2018 provisions and similar models have been adopted by the Internet Courts in Beijing and Guangzhou[38].

The technique used in China requires hashing and timestamping of real evidence on a blockchain as soon as it is created to prove the deepfake is authentic. Any subsequent deepfake video that doesn't appear on the data blockchain-supported registry can be identified as a fake, as it's not part of the ledger, for instance. This approach isn't foolproof, because a hacker who had access to the recording system could upload a fake file before the hashing process was performed, but the steps involved in the process are significant. This is a vastly different way of certifying than the post event methods that currently depend on in India.

The defects of the Chinese model on the democratic aspect have been much debated. With platforms managed by the state, compulsory real name registration, and a lack of independent

[36] Deep Synthesis Provisions, *supra* note 9, arts. 17—18 (mandating labelling and log retention).
[37] Interim Measures for the Management of Generative Artificial Intelligence Services (promulgated by Cyberspace Admin. of China et al., July 13, 2023, effective Aug. 15, 2023) (China), arts. 4, 12.
[38] Huatai Insurance v. Huayuan Tech., (2018) Zhe 0192 Min Chu No. 81 (Hangzhou Internet Ct., June 28, 2018); *see also* Supreme People's Court of the People's Republic of China, Provisions on Several Issues Concerning the Trial of Cases in Internet Courts (Sept. 7, 2018), art. 11 (recognising blockchain-authenticated electronic evidence).

judicial oversight, the possibility of applying this model to a constitutional democracy becomes problematic. India is not in a position to fully replicate the Chinese system, not should it attempt to do so. The basic idea that cryptographic verification at the time of recording offers greater reliability than validation afterward – is valid and can feasibly fit within India's current constitutional structure.

D. A Framework for India

A combination of these three models indicates a four part reform plan for India. For starters, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, need to be modified to require creators and intermediaries of artificially intelligent content to label their work. This adjustment should take inspiration from Article 50 of the European Union Artificial Intelligence Act while being tailored to align with India's intermediary liability framework outlines in Section 79 of the Information Technology Act, 2000. The advisories issued by the Ministry of Electronics and Information Technology[3940] in November 2023 and March 2024 already suggest this direction, although they currently serve as recommendations only.

There should be a revision of the Bharatiya Sakshya Adhiniyam, 2023, to add a new section. It should focus on the acceptance of synthetic media. Under this provision, the person promoting the media must reveal any known generative processing, the opposing party should have the right to review the metadata and the court should have the authority to send disputed media for expert review.

In addition to this, an accredited network of deepfake forensic labs should be created under the India Computer Emergency Response Team, similar to the current model for NABL, accredited DNA labs. Finally, the National Judicial Academy along with State Judicial Academies must indicate generative artificial intelligence training in their required training programs[41].

[39] Ministry of Electronics & Information Technology, Govt. of India, Advisory to Intermediaries (Mar. 1, 2024), and revised Advisory (Mar. 15, 2024) [hereinafter MeitY Mar. 2024 Advisory], available at https://www.meity.gov.in.
[40] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S.R. 139(E) (Feb. 25, 2021), as amended by G.S.R. 794(E) (Oct. 28, 2022) and G.S.R. 275(E) (Apr. 6, 2023).
[41] On the imperative of judicial training in the era of generative AI, *see* Indian Judiciary, Supreme Court of India, *Annual Report 2023—24*, at 87—89 (discussing AI literacy initiatives at the National Judicial Academy, Bhopal).

IV. CONSTITUTIONAL DIMENSIONS

The challenges in evidence arising from deepfakes extend beyond procedural aspects. They involve at least three sections of Part III of the Constitution of India and, with a more conjectural interpretation, potentially a fourth.

The first is Article 21. In the case of Maneka Gandhi Vs Union of India[42], the Supreme Court established that any process leading to the deprivation of a person's life or personal freedom must meet the standards of being *"fair, just and reasonable, not fanciful, oppressive or arbitrary."*[43] The concept of a fair trial which includes equality of arms, the ability to confront evidence and the right to rely on credible proof has firmly been integrated into Article 21. A conviction based on a deepfake that has not undergone sufficient verification is inherently unjust ; the defendant is found guilty based on a fabrication that the procedural law does not require to authenticate.

The remarks made by the Supreme Court in Tomaso Bruno Vs State of Uttar Pradesh[44] regarding the importance of CCTV evidence in contemporary criminal proceedings gain new relevance in this context. If electronic records are to hold significant evidentiary value, the procedural law needs to be adjusted to identify synthetic evidence. Without this, Article 21 is breached not by lack of evidence, but by the failure to validate it. Furthermore, the reasoning from the same Court in State of Maharashtra Vs Praful B. Desai[45], which addressed how procedural law can adapt to new technologies particularly in the context of video conference testimonies, provides a theoretical basis for the opposite argument – that procedural law must also be able to retract when faced with reliable new technology.

The second point is Article 20(3), which guarantees that no individual facing charges can be forced to testify against themselves[46]. Traditionally, the main issue with the right against self-incrimination revolves around the pressure to provide testimony. However, with the rise of

[42] Maneka Gandhi v. Union of India, (1978) 1 SCC 248, 284 (India) (Bhagwati, J.).
[43] *Id.* at 284 (para 7). The standard has since been reiterated in Mohd. Arif v. Registrar, Supreme Court of India, (2014) 9 SCC 737 (India).
[44] Tomaso Bruno v. State of U.P., (2015) 7 SCC 178, 196—97 (India) (observing that non-production of available electronic evidence may attract adverse inference in a criminal trial).
[45] State of Maharashtra v. Praful B. Desai, (2003) 4 SCC 601 (India) (recognising video-conferencing evidence and the constitutional capacity of procedural law to adapt to technology).
[46] Constitution of India, art. 20(3).

generative artificial intelligence, a different type of pressure has emerged. An artificially generated confession could be placed on the accused device or represented by Voice-cloned audio, making it possible to use this against them without them ever having uttered a word.

In the case of Selvi Vs State of Karnataka, a three-judge panel established that conducting narco-analysis, polygraph tests and brain mapping without consent infringes on both Article 20(3) and Article 21[47]. The principal behind the ruling was that the State cannot obtain self-incriminating evidence through technological means without consent. This clearly applies to deepfakes as well. If a court allows an artificial generated confession video as evidence without strict verification, it effectively undermines the accused identity as the origin of the testimonial evidence. But whether Article 20(3) has been violated directly or indirectly by Article 21 and evidentiary laws is a doctrinal question with shades of nuance. However, the constitutional issue is apparent.

The third point pertains to Article 14 which ensures equal protection under the law, specifically concerning the procedural law of evidence. The forensic analysis of deepfakes incurs significant costs. In the current Indian context, a dependable expert examination of a disputed video comprising of spectral analysis, biological signal detection, GAN fingerprinting and a written court admissible report costs anywhere between two lakhs to ten lakhs. International consultations can be substantially more expensive. Those who can afford such analysis can contest the States evidence on an equal footing. Conversely, defendants lacking financial resources depend on the trial court's willingness to order an independent examination as per Section 39 of the Bharatiya Sakshya Adhiniyam, 2023, a privilege that is seldom granted in practice. This situation leads to procedural disparity that is influenced by wealth, which aligns with the type of inequality that Article 14, in conjunction with Article 21, has been interpreted to prohibit since the Maneka Gandhi case and further reinforced in Hussainara Khatoon (4) Vs Home Secretary, State of Bihar[48]. A potential solution exists : legal aid provisions from the Legal Services Authorities Act, 1987, could be expanded to include coverage of forensic analysis expenses for dependents without

[47] Selvi v. State of Karnataka, (2010) 7 SCC 263, 382 (India) (Balakrishnan, C.J.).
[48] Constitution of India, art. 14, read with art. 21; *see also* Hussainara Khatoon (4) v. Home Secretary, State of Bihar, (1980) 1 SCC 98 (India) (free legal aid is integral to fair trial under Article 21).

financial means[49]. Nevertheless, achieving this requires statutory or administrative measures as it will not occur automatically.

The fourth, interconnected dimension relates to Article 19(1)(a) and the chilling effect that concerns over deepfakes may impose on valid speech. In the case of Shreya Singhal Vs Union of India[50], the Supreme Court acknowledged that a broad criminalization of online expressions can deter the realization of fundamental rights. Similarly, the rise of synthetic media may inhibit individuals from expressing themselves authentically as their genuine content risks being labeled as fake. This phenomenon reflects the idea of the liar's dividend as it intersects with free expression. Although this discussion is not elaborated upon here, it is important to note that a cohesive regulatory approach to deepfakes must address both sides of the speech spectrum ; the individual whose likeness is wrongfully used and the individual whose authentic voice is dismissed. The Delhi High Court has recently issued a ruling in Anil Kapoor Vs Simply Life India (Anil Kapoor v. Simply Life India, 2023 SCC OnLine Del 6914 (India) (Pratibha M. Singh, J.)), highlighting the dangers of relying on information acquired on social media. An analogous injunction in Jaikishan Kakubhai Saraf v. Peppy Store, 2024 SCC OnLine Del 3664 (India) (for the recognition of actor's personality rights and granting an injunction against deepfake exploitation) provides a positive yet limited solution to the first aspect of this issue; while the latter still needs a systematic legal framework.

V. CONCLUSION AND RECOMMENDATIONS

The central argument of this paper is that the Bharatiya Sakshya Adhiniyam, 2023, which is promoted as a modernization of evidence law in India, is not adequately equipped for the challenges presented by generative artificial intelligence. While the certification process outlined in Section 63 focuses on verifying sources, it fails to address the verification of content. Additionally, the surrounding legal framework including the Information Technology Act, 2000, the Intermediary Rules of 2021 and various advisories from the Ministry of Electronics and Information Technology does not adequately bridge this gap. The implications for the constitution are significant, the protections offered by Article 21 for a fair trial, Article 20(3) against self-

[49] Legal Services Authorities Act, 1987, No. 39, Acts of Parliament, 1987 (India), §§ 12, 13.
[50] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).

incrimination, and Article 14 concerning equal procedural safeguards are in conflict with the existing evidentiary framework.

What is required is a coordinated program of reform on five fronts.

First – It is proposed that a new section be added to address synthetic media. This section should require the party presenting digital evidence to reveal any artificial intelligence processing that is known or reasonably suspected to have been applied to the evidence. In addition to this, the court should have the authority to mandate a pre-trial cryptographic examination of metadata. Furthermore, there should be a rebuttable presumption against the acceptance of evidence if its synthetic origin is credibly claimed as this presumption should remain until the presenting party meets a higher standard of authentication. The drafting of the section should make it clear that the function of section 63, which is authentication of source, remains unaffected, and that this new section should be thought of as a layer for authentication of content.

Secondly – that the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rule 2021 be amended to make it mandatory on the part of major social media intermediaries to apply the C2PA standard watermarks to artificially generated content. They should also maintain provenance information for a certain period of time (at least six months in accordance with the regulations of the Chinese government) and be obligated to release this information when the court requests. The advisory status of the November 2023 and March 2024 guidance notes issued by the Ministry of Electronics and Information Technology should be changed to mandatory with teeth under Section 79(3)(b) of the Information Technology Act.

Third – the Indian Computer Emergency Response Team should collaborate with the Central Forensic Science Laboratories and the National Forensic Sciences Universities to create a network of certified deepfake analysis centers. This certification ought to rely on clear technical standards released by the Bureau of Indian Standards. In addition to this, Laboratories must reveal their methodologies, error rates and data sourcing, aligning with the principles of the Daubert standard. A fitting example is the framework of NABL – accredited DNA testing facilities, which has developed over the last twenty years and now provides the court with fairly dependable forensic evidence.

Fourth – the National Judicial Academy in Bhopal, along with the State Judicial Academies ought to include modules covering generative artificial intelligence, deepfake education program for trial and appellate judges. Even the most sophisticated forensic systems will fail without judges that are well-trained to act as gatekeepers. This is the case in the United States after Daubert, where individual District Judges have exhibited considerable variations in their willingness and ability to perform the role of gatekeeper.

Fifth – it is necessary to amend the Legal Services Authorities Act of 1987 or alternatively the National Legal Services Authority should provide administrative guidance based on its current authority to ensure that accredited deepfake analysis is accessible to low income defendants just as legal representation is. Article 14 requires this equality and the Supreme Court's rationale in Hussainara Khatoon offers a solid doctrinal basis for it.

This paper does not cover several important questions that deserve further investigation. A thorough examination is necessary to understand how new proposed section that addresses synthetic media interacts with the Secondary evidence regulations found un Sections 60 to 65 of the Bharatiya Sakshya Adhiniyam, 2023. Moreover, the role of generative artificial intelligence in Indian laws pertaining to identification and recognition evidence, especially with regards to Section 27 of the Bharatiya Sakshya Adhiniyam, 2023, which corresponds to the earlier Section 27 of the Indian Evidence Act, remains largely unexamined. Furthermore, the employment of generative artificial intelligence by investigative agencies whether for enhancing evidence, reconstructing witness testimonies or engaging in predictive policing, raises unique constitutional issues, which while related, do not directly align with the evidentiary concerns addressed in this study. In addition to this, the international aspect involving mutual legal assistance, cross border data preservation and the acceptance of foreign deepfake forensic reports is also insufficiently explored. Each of these topics present an independent research opportunity.

Clearly, the period of lawmakers' inaction is over. Today's legal tools have already been overcome with the development of synthetic media. This was an opportunity for the Parliament to address the issue, as presented in the Bharatiya Sakshya Adhiniyam, 2023, but it was not taken. In the interim, Indian Courts will continue to encounter deepfake evidence – sometimes directly contested, but more frequently accepted without challenge, as no one in the courtroom thinks to

question its authenticity. These are just some essential reforms that are suggested in this location, but they do not necessarily refer to everything. Otherwise, the justice system runs the risk of continuing to uphold the notion that “seeing is believing”, because the courts have not yet caught up to what is now possible to discern.