INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 6 AND ISSUE 3 OF 2026

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

REGULATING SYNTHETIC VOICE IMPERSONATION IN COURTS: A COMPREHENSIVE RESEARCH PAPER WITH INDIAN LEGAL FRAMEWORK

AUTHOR - MANAN JHAMB, STUDENT AT CHANDIGARH UNIVERSITY

BEST CITATION – MANAN JHAMB, REGULATING SYNTHETIC VOICE IMPERSONATION IN COURTS: A COMPREHENSIVE RESEARCH PAPER WITH INDIAN LEGAL FRAMEWORK, *INDIAN JOURNAL OF LEGAL REVIEW (IJLR)*, 6 (3) OF 2026, PG. 352-361, APIS – 3920 – 0001 & ISSN - 2583-2344. DOI - https://doi.org/10.65393/UOUQ6138

I. UNDERSTANDING THE TOPIC: EXPLAINING

Concept: Synthetic Voice Impersonation

Artificial Voice Impersonation is when systems or people are deceived into thinking that an artificially created voice — produced by AI and Deepfake technology — is a genuine individual's voice. In literature the fake voice creation process is called synthetic voice cloning or voice synthesis; AI algorithms are trained on a set of previously recorded voices to create vocalizations that mimic the tone of the training sample. The hyper-realism of these artificially created audio reproductions makes them nearly indistinguishable from actual human voices; thus, there are problems associated with deception and digital consent.[982] There is documented evidence of the use of fabricated/impersonated synthetic voice in committing crimes and fabricating evidence. Thus, there is a very serious problem for Courts of Law — in which the presentation of fabricated audio recordings can be used as "evidence" to support claims of confessions from defendants or statements from witnesses or victims; therefore, the reliability of the trial being fair cannot be ensured and the integrity of the evidence has been questioned.[983]

[982] Kumar, R. (2025). Synthetic voice impersonation technology and the "Liars Dividend": Regulatory gaps and comparative legal safeguards. Asian Journal of Law and Technology, 11(2), 177–210

[983] Kothari, V., & Tibrewala, A. (2024). Synthetic voice impersonation as a threat to judicial integrity and fair trial rights. Journal of Digital Forensics, Security and Law, 19(4), 87–109.

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

- **Mechanism**

Deep learning models such as WaveNet and Taco Tron are being used to create artificial voices for use by developers in creating synthetic voice models that can be used to synthesize voice audio recordings based on large data sets of human speech to mimic the pattern of speech of humans.[984]The importance of regulating synthetic voice impersonation in courts

a. Threats to judicial integrity

Synthetic voice impersonation in courts threatens the integrity of the Indian judiciary at a minimum. It compromises the evidentiary value of audio in courts and thus the right to a fair trial which is guaranteed by Article 21 of the Indian Constitution. In other words, "audio evidence is sacred," however, we are unable to distinguish between authentic audio recordings and those created using AI.[985]

- **Evidentiary Challenges in Indian Courts**

Prior to the BSA 2023 India's laws regarding all types of digital evidence was shrouded in uncertainty for how they would be interpreted by the courts. It seemed that this uncertainty continued until the creation of the Bharatiya Sakshya Adhiniyam (BSA), 2023; the BSA intended to overhaul and possibly change aspects of the procedures involved with submitting digital evidence in court.[986] Evidently, synthetic voice impersonation has been one of the many variables that the BSA did not consider at its inception, primarily due to the new deepfake technologies that have developed.

- **Criminal Law Implications**

In criminal jurisprudence, synthetic voice impersonation can be used to commit serious crimes such as creating a belief that should never have been created with regard to confessions made by an individual, or perhaps worse still, utilizing deep fake project voice to create doubt regarding a guilty party[987] synthetic voice manipulation of an individual's voice – if it is even possible to understand a synthesized voice as truly at a one remove from the visage of a human object through deep fake technology[988], is a crime that falls somewhere between fraud and forgery, therefore we need as a legal society to define the fine lines within that definition of a deep fake user.

Impact on Democratic Institutions and Public Trust

Synthetic voice impersonation also jeopardizes the overall credibility of the entire legal system in India. If citizens start to question whether audio presented in court is authentic, the judiciary's general credibility is compromised. This creates what is known as the "Liars Dividend," where even real evidence may be treated with suspicion as potentially being manipulated, thus undermining the evidentiary system.[989]

INDIA'S CURRENT LEGAL FRAMEWORK AND GAPS, EXISTING INDIAN LEGISLATIVE PROVISIONS

- **The Information Technology Act, 2000**

The primary legislation in force today is the IT Act of 2000 and it does have provisions regarding cybercrime in general terms, however, it doesn't provide legal punishment for creation and distribution of fake audio recordings to be used against an individual, or even those that are intended to be presented as evidence in courts.[990]

[984] Wu, Y. (2025). Deep learning models (WaveNet and Tacotron) for synthetic voice replication and vocal characteristic modeling. IEEE/ACM Transactions on Audio, Speech, and Language Processing, 33, 512–528

[985] Kothari, V., & Tibrewala, A. (2024). Synthetic voice impersonation as a threat to judicial integrity and fair trial rights. Journal of Digital Forensics, Security and Law, 19(4), 87–109

[986] Goyal, R., & Mali, P. (2025). Evidentiary challenges in Indian courts: Integration with digital evidence frameworks and cross-border digital evidence concerns. Indian Journal of Law and Technology, 21(1), 55–82

[987] Sayyed, M. (2024). Criminal offenses facilitated by synthetic voice impersonation and attribution of liability in AI-generated content. Journal of Criminal Law & Criminology, 114(3), 521–548

[988] Khokhlova, E. (2025). Criminal implications of synthetic voice impersonation through deepfake technology. European Journal of Criminal Law and Cybersecurity, 12(3), 201–226

[989] Kumar, R. (2025). Synthetic voice impersonation technology and the "Liars Dividend": Regulatory gaps and comparative legal safeguards. Asian Journal of Law and Technology, 11(2), 177–210

[990] Kumar, R. (2025). Synthetic voice impersonation technology and the "Liars Dividend": Regulatory gaps and comparative legal safeguards. Asian Journal of Law and Technology, 11(2), 177–210

- **The Bharatiya Nyaya Sanhita, 2023**

The BNS of 2023 is India's new Criminal Code that replaces the IPC of 1860. While the 2023 BNS has created improved provisions to address several types of cybercrime, the BNS fails to adequately cover the complex nature of synthetic media as a threat, specifically voice impersonation used for the purpose of legal proceedings (Kumar, 2025).

- **The Bharatiya Sakshya Adhiniyam, 2023**

The 2023 BSA has updated India's legal standards regarding evidence. The Act provides clarification on certain aspects of the process-related rules governing digital documents. In addition, the Act expands the definition of "document" to also encompass electronic records.[991] For example, sections 61 and 63 of the BSA are both specifically focused on the admissibility of electronic records and expert certification, however, the BSA does not explicitly mention or even remotely address the issues surrounding the use of AI-generated voice as evidence in court proceedings, which is creating a significant regulatory gap.

- **The Critical Gap: Absence of Specific Deepfake Voice Legislation**

India is one of a number of western countries that has yet to enact specific legislation criminalizing the creation and circulation of fake audio content using deepfakes.[992] In contrast, the United States has enacted statutes including the No Fakes Act and the Defiance Act, while the U.K.'s Online Safety Act 2023 criminalizes the sharing of non-consensual explicit deepfakes; in India the law relies upon more general provisions which do not effectively capture the complexities of deepfake audio impersonations.[993]

- **Forensic and Investigative Limitations**

Deepfakes are a new technology that has developed at an accelerated rate, it is therefore understandable that there is currently no recognized standards or processes for detecting them. A recent report from the Global Forensic Science Symposium identified that while the Indian Government has made significant progress in developing forensic science, the country still requires improved technical infrastructure and capacity, particularly with respect to the detection of digital audio and video evidence (Singh, 2023). Furthermore, the use of chain-of-custody procedures to protect integrity of digital evidence is also very limited; as well as limited communication between law enforcement agencies and forensic experts, which can limit their ability to evaluate and utilize synthetic media evidence (Singh, 2023).

SYNTHETIC VOICE IMPERSONATION IN CRIMINAL JUSTICE: SPECIFIC VULNERABILITIES

- **Undermining Right to a Fair Trial**

The use of synthetic voice evidence in criminal trials presents unique challenges to the right to an unobstructed fair trial, which is a right granted to all citizens through Article 21 of the Indian Constitution. In cases where deep-fake audio allegedly contains a confession or an incriminating statement made by the defendant, the authenticity of the evidence itself is a major issue. Without reliable tools for detecting synthetic audio and clear legal standards that define what constitutes authentication, the burden falls upon the accused to prove that the audio was fabricated.[994]

- B. EVIDENCE TAMPERING AND CHAIN OF CUSTODY ISSUES

The concept of chain of custody is important for physical evidence as well; however, chain of custody is much less relevant when dealing with digital audio. A single digital file can be edited multiple times before it reaches the courtroom, starting at the time of recording, through storage, and up to presentation as evidence. Present day software is capable of creating

[991] Singh, A., et al. (2025). Electronic records authentication under the Bharatiya Sakshya Adhiniyam, 2023: Evidentiary standards for audio evidence. Journal of Indian Law and Society, 16(1), 91–118

[992] Kumar, R. (2025). Synthetic voice impersonation technology and the "Liars Dividend": Regulatory gaps and comparative legal safeguards. Asian Journal of Law and Technology, 11(2), 177–210

[993] Kumar, R. (2025). Synthetic voice impersonation technology and the "Liars Dividend": Regulatory gaps and comparative legal safeguards. Asian Journal of Law and Technology, 11(2), 177–210

[994] Kothari, V., & Tibrewala, A. (2024). Synthetic voice impersonation as a threat to judicial integrity and fair trial rights. Journal of Digital Forensics, Security and Law, 19(4), 87–109

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

sophisticated fakes of digital files including audio, and typical procedures for handling digital evidence in India are not keeping pace.[995]

- C. PROBLEM OF THRESHOLD OF AUTHENTICITY

Researchers have identified that even experienced forensic audio reviewers have difficulty determining whether an audio sample is authentic or not synthetic.[996] The researchers conducted a study testing participants' ability to accurately identify deep-fake audio files. While the participants were able to accurately identify approximately one-third of the deep-fake audio samples, they were unable to accurately identify approximately one-third of the actual (authentic) audio files (i.e., those that could have been identified by a legitimate means of detection). This study resulted in a false positive rate for the new problem created by deepfakes — called "the Liar's Dividend" by academic scholars.[997]

- V. VOICE BIOMETRICS AND JUDICIAL AUTHENTICATION

Voice as Biometric Evidence

The use of voice as a biometric technology to identify individuals based on the individual's voice patterns, frequency of voice effects and other characteristics has been considered by the courts.[998] Unfortunately, the same biometric technique of identifying individuals based on their voices is susceptible to deepfakes as well. If a voice is mimicked to sound like a witness, then the jury may believe that the synthesized version of the voice is authentic and therefore the audio fake will convince the judge.[999]

- **Mitigation: multi-factor and multi-agency verification systems**

A possible method of counteracting spoofing would be the utilization of multi-modal or multi-entity authentication methods that include various modalities such as; voice biometrics, facial micro-movements, other data (IP address, device, time, etc.), liveliness detection and so on. The combination of all these different types of modalities makes it much more difficult for a potential fraudster to game the simple system of an individual entity.[1000]

A COMPARATIVE AND INTERNATIONAL SYNOPSIS OF DEEPFAKE RESPONSES FOR THE INDIAN COURT SYSTEM

While the regulatory approaches to addressing deepfakes differ, the U.S. and Indian regulatory frameworks have taken a piecemeal approach to regulating the use of deepfakes; however, the U.S. has taken a much more fragmented approach than India in addressing this issue. The "No Fakes Act" addresses federal concerns with election fraud and misinformation, and states have their own laws targeting sexual harassment (Kumar, 2025). However, there does appear to be a void in the current regulation of deepfakes intended to undermine justice. The UK has adopted an online safety act of 2023 as a piecemeal approach to regulate illicit non-consensual deepfakes of mainly sexual images, and it has been used to regulate justice-related nefarious uses. The UK method of developing specific deepfake legislation to find a balance of protecting artistic freedom and parody is something India should study (Kumar, 2025) .

India's Unsatisfactory Attempt.

India has no legislation that specifically provides criminal sanctions to punish someone who creates a fake voice or distributes it for the purpose of fraud, particularly in a judicial context; unlike some states of America and the United Kingdom (Kumar, 2025) where there are laws regarding this issue. The BNS, 2023, and the Information Technology Act, 2000, do not provide enough protection to ensure justice in

[995] Goyal, R., & Mali, P. (2025). Evidentiary challenges in Indian courts: Integration with digital evidence frameworks and cross-border digital evidence concerns. Indian Journal of Law and Technology, 21(1), 55–82

[996] Rodgers, J., et al. (2024). Forensic audio professionals' ability to distinguish authentic from synthetic voice samples: False positive risks and the "Liars Dividend." Science & Justice, 64(5), 402–417

[997] Rodgers, J., et al. (2024). Forensic audio professionals' ability to distinguish authentic from synthetic voice samples: False positive risks and the "Liars Dividend." Science & Justice, 64(5), 402–417

[998] Ouahab, L., et al. (2024). Voice biometric technology as evidence in legal proceedings. Forensic Science International: Digital Investigation, 48, 301–318

[999] Smanova, D., et al. (2025). Vulnerability of voice biometrics to deepfake attacks and authentication reliability concerns. IEEE Access, 13, 45567–45584

[1000] Gunzo, T., et al. (2025). Multi-factor verification systems combining voice biometrics with facial micro-motion analysis and liveness detection. Computers & Security, 134, 103211

cases of using deepfakes to cheat.

DETECTION AND FORENSIC MECHANISMS

- **Technology-Based Detection**

Promising research involves the use of Spectro-Temporal Analysis techniques and CNNs/RNNs for detecting Deep Fake Audio by examining specific aspects of the audio in terms of spectrogram information with an aim to identify anomalies that could indicate the use of AI in creating the audio.[1001] Another method of detection is to analyze the harmonic structure and formants which are difficult to recreate with synthetic voice [1002]

- **AI Detection Classification Models**

In addition to the above, binary classification using CNN-BiLSTM models with ensemble learning classifiers have reached >99% accuracy for dataset sizes greater than 2,000 samples[1003]— which indicates that this type of tool may eventually be created. However, at present, there are many barriers to implementing such technology within Indian Courts including, but limited to, requiring substantial investment in infrastructure, officer training, and interfacing with the existing software being used to manage evidence in cases such as CCTNS and ICJS.[1004]

V. Limitations and Adversarial Robustness Challenges

Although there has been considerable technological advancement regarding the development of deepfake detection systems, these systems can still be vulnerable to adversarial attacks — specifically, adversarial designed audio intended to deceive detection algorithms.[1005] As a result of this adversarial aspect, we see an ongoing "arms race" between the developers of artificial speech and those developing the detection systems required to identify it; a challenge that India's forensic infrastructure is unlikely to be capable of addressing currently.[1006]

THE WITNESS' KIDNAPPED

- **Criminal Liability and Accountability**

A. Who Takes the Fall for a Murderous Faux-Pas?

Who gets blamed when a crime is done with this technology? The sad school dropout who got fired and now he's broke? Clearly there is an enormous need for packaging here and figuring out which one of those packages (synthesizer, the tweaking voice, the voice recognizer, or the package that the system uses to play back what the listener may end up dying from) should be blamed? In its current state, India has no criminal law that addresses "who is guilty" of making it appear like the original.[1007]

B. A Model for True Crime! Offenders

As the Russian criminal corpus has shown in Russia and as we are finding out here in the US, legislation can help protect people from losing their right to receive protein and vitamins; and in Russia, legislation concerning a new bill appears to be a relatively easy one to add to the list of the other fake voice generated voices[1008] in Russia. India should include language that specifically defines offenses of proprietary creation of audio/video voice record(s) for deceptive purposes against judges and magistrates, similar to what was done in Russia.

EVIDENTIARY STANDARDS AND PROCEDURAL REFORMS

- **The New Kid on the Block**

Are the witnesses comprised of 100% organic material? And what are the odds that we should accept the truth of their testimony? The providers of the BSA, 2023 will claim that all electronic records require certification along

[1001] Srinagesh, K. (2024). Spectro-temporal analysis for synthetic voice detection using CNNs and RNNs. Digital Signal Processing, 144, 104202
[1002] Williams, T., et al. (2025). Harmonic structures and formant pattern analysis in synthetic voice identification. Speech Communication, 167, 112–129
[1003] Deshpande, A., et al. (2025). Machine learning-based classification models for deepfake audio detection with CNN-BiLSTM architecture. IEEE Transactions on Information Forensics and Security, 20(4), 789–804
[1004] Goyal, R., & Mali, P. (2025). Evidentiary challenges in Indian courts: Integration with digital evidence frameworks and cross-border digital evidence concerns. Indian Journal of Law and Technology, 21(1), 55–82
[1005] Chandrapalan. (2025). Adversarial robustness challenges in deepfake detection systems. International Journal of Artificial Intelligence Security, 9(1), 33–59
[1006] Singh, A., et al. (2025). Electronic records authentication under the Bharatiya Sakshya Adhiniyam, 2023: Evidentiary standards for audio evidence. Journal of Indian Law and Society, 16(1), 91–118
[1007] Sayyed, M. (2024). Criminal offenses facilitated by synthetic voice impersonation and attribution of liability in AI-generated content. Journal of Criminal Law & Criminology, 114(3), 521–548
[1008] Mosechkin, I. (2025). Falsification of biometric data through AI systems in Russian criminal jurisprudence. Russian Law Journal, 13(1), 64–92

with expert authentication,[1009] but if there is a hacking death of a witness then it might be time to create an e-witness box that has at least one reader capable of reading the morse code that represents "fox trot" golf to hear and recognize your well-plated in craspberry? Rubbish! India will need to develop new evidentiary standards which would include that records be as follows:
1. As assured by forensic experts – a certificate with evidence to support who authored the record.
2. Chain of custody as others have already shown to be convincing to meet international standards.
3. Independent expert testimony from audios.
4. An author dressed as a cleverly disguised anorak wearer sufficiently to analyze other testable samples as other samples.

- **Cross-Border Digital Evidence Challenge**

The majority of deepfakes originate from foreign jurisdictions, and thus, there are jurisdictional challenges to collecting evidence and investigating offenses in the digital domain as well as providing for the transnational dimensions of such crimes in the legal framework of India, possibly by way of bilateral agreements or through cooperation with international law enforcement organizations [1010]

PRIVACY AND HUMAN RIGHTS CONSIDERATIONS

- **Privacy Rights Regarding Voice Data**

Privacy was held as a fundamental right of every Indian citizen through the K.S. Puttaswamy v. Union of India case in the Supreme Court and the Court's ruling imposed the Constitutional obligations of preventing unauthorized collection and misuse of voice data. Thus, any Regulatory Framework that will be to govern Synthetic Voice Impersonations will have to maintain a balance between fulfilling the need to detect crimes using this type of fraud against the privacy rights of the citizens.[1011]

- **Data Protection Issues**

Because the Digital Personal Data Protection Act of 2023 (DPDPA), which is the Indian law regulating how companies must handle personal data, does protect biometric data, India's law for protecting privacy rights should be changed to include the voice in addition to other forms of biometric data as something that is regulated by DPDPA, and provide increased penalties for synthesizing someone else's voice.

- **Obtaining Informed Consent for Voice Authentication**

The use of voice biometrics in judicial applications has sparked discussion on how to obtain voluntary and informed consent from individuals when their voices will be recorded. As an example, those who record their voice through video conferencing service or testimony devices must be knowledgeable of the possibility that their recorded voice can be manipulated into a digital imitation (deep fake) and therefore consent to the recording of their voice for this purpose; and therefore require transparency as well as a system of consent to be able to minimize the potential misuse of these recordings.[1012]

- **PROPOSED LEGISLATIVE REGIME FOR INDIA**

- **Enactment of Specific Legislation Addressing Deepfake Audio in Judicial Proceedings**

Specific legislation should be created in India to create a criminal offense for creating or distributing synthetic voice recordings of an identifiable individual with the intent to impersonate that person. Legislation should also include provisions to increase penalties for the creation or distribution of synthetic voice recordings of identifiable individuals. In addition

[1009] Singh, A., et al. (2025). Electronic records authentication under the Bharatiya Sakshya Adhiniyam, 2023: Evidentiary standards for audio evidence. *Journal of Indian Law and Society*, 16(1), 91–118
[1010] Goyal, R., & Mali, P. (2025). Evidentiary challenges in Indian courts: Integration with digital evidence frameworks and cross-border digital evidence concerns. Indian Journal of Law and Technology, 21(1), 55–82
[1011] Goyal, R., & Mali, P. (2025). Evidentiary challenges in Indian courts: Integration with digital evidence frameworks and cross-border digital evidence concerns. Indian Journal of Law and Technology, 21(1), 55–82
[1012] Pathak, N., et al. (2025). Informed consent in voice authentication and voice data disclosure frameworks. Computer Law & Security Review, 49, 105812

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

to increasing the penalty for the creation and distribution of synthetic voice recordings of identifiable individuals, specific legislation should be created to provide for evidentiary standards for determining whether digital evidence (audio) is authentic, and for the procedures that require forensic certification and expert testimony prior to allowing digital evidence (audio) to be admitted into evidence during a judicial proceeding.

- **Amendments to the Bharatiya Sakshya Adhiniyam, 2023**

The Bharatiya Sakshya Adhiniyam, 2023 should be amended to include provisions addressing:
1. Sections of law that specify the process for authenticating deepfake audio;
2. Presumptions of authenticity for audio evidence that may only be rebutted if certified forensic analysis of the evidence is produced;
3. Expert qualifications for audio forensics specialists;
4. Chain of custody procedures that are tailored for digital audio evidence.

C. Amendments to the Criminal Procedure Code

The Criminal Procedure Code should be amended to include:
1. Investigative protocols for investigating deepfake-related complaints;
2. Standards for forensic examination of audio evidence;
3. Guidelines for judges on evaluating synthetic media evidence;
4. Mechanisms to protect defendants challenging audio evidence as deepfakes.

DEVELOPING INSTITUTIONAL CAPACITY

- **Developing Forensic Laboratory Capacity for Audio Analysis**

India must improve its forensic laboratory infrastructure to analyze audio evidence, specifically to detect deepfakes:
1. Establish specialized audio forensic units in major forensic science laboratories (FSLs);
2. Develop standardized methodologies for detecting deepfakes;
3. Obtain international accreditation (ISO 17025) for audio forensic work;
4. Establish inter-laboratory collaboration networks to facilitate analysis of complex cases.

- **B. Providing Judicial Training**

Judges must receive comprehensive training on:
1. Modules on deepfake technology and evidence evaluation at judicial academies;
2. Specialized training for judges who preside over cases involving synthetic media evidence;
3. Regular updates on evolving methodologies for detecting deepfakes;
4. Case law analysis of how courts in other countries have dealt with synthetic audio evidence.

- **Enhancing Inter-Agency Collaboration**

To effectively regulate the use of deepfakes in India, effective collaboration among:
1. Central and State FSLs;
2. Law Enforcement Agencies (Police, CBI, etc.);
3. Judiciary;
4. Organizations protecting digital rights;
5. Technology Companies;
6. Academic Institutions;
is necessary.

INTERNATIONALLY ACCEPTABLE STANDARDS AND HARMONIZATION

- **The Budapest Convention and Deepfakes**

Although India is not currently a party to the Budapest Convention on Cybercrime, the lack of explicit references to deepfakes in the Convention does not preclude India from relying on the Convention's framework on cybercrime investigations to guide its efforts to develop policies and regulations to address the use of deepfakes. Moreover, India should seriously consider becoming a party to the Convention and participating in the development of supplementary protocols specifically dealing with synthetic media.[1013]

- **Protocols for Cross-Border Investigations**

When deepfakes created abroad are introduced into Indian courts, India must have mechanisms for cross-border investigations

[1013] Beaver. (2025). Budapest Convention and deepfake gaps: Cross-border investigation protocols. Journal of Cybercrime & Digital Evidence, 14(2), 145–168

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]
VOLUME 6 AND ISSUE 3 OF 2026
APIS – 3920 - 0001 *(and)* ISSN - 2583-2344
Published by
Institute of Legal Education
https://iledu.in

and gathering of evidence. As a result, Mutual Legal Assistance Treaties (MLATs) should be revised to include deepfake crimes, and standardize protocols for forensic examinations and evidence authentication.[1014]

- **Harmonizing International Regulations**

Although India cannot achieve complete harmony in regulating the use of deepfakes, India should align its regulatory approach with international best practices:
1. Adopt standardized methodologies for detecting deepfakes that are acceptable within the global community of forensic scientists;
2. Align qualification requirements for experts in audio forensics with international standards for such expertise;
3. Harmonize evidentiary standards for digital audio evidence;
4. Participate in international working groups on regulating the use of synthetic media.

PRACTICAL CHALLENGES AND ISSUES OF IMPLEMENTATION

- **The Paradox of Detection Technology**

One of the principal challenges facing India's regulatory efforts is that the technologies used to detect deepfakes are rapidly evolving. However, the same applies to the technologies used to create deepfakes. As a result, by the time courts and forensic labs become proficient in detecting one generation of deepfakes, the next generation of deepfakes will have evolved beyond recognition, thereby rendering prior detection technologies ineffective.[1015] Consequently, India must continuously invest in R&D to stay ahead of the curve, create organizational structures that allow for rapid adaptation to changing detection technologies, and train judges to be aware of the constant evolution of both detection and synthesis technologies.

- **B. The Robustness of Detection Algorithms**

As deepfake creators evolve to defeat detection algorithms through the use of adversarial techniques, the technological battle to defeat deepfakes becomes an arms race that no single court, or even national forensic system, can win.[1016] Consequently, India must collaborate with globally connected research institutions to continue to advance the state-of-the-art in detecting deepfakes.

- **False Positives and False Negatives**

False positives (i.e., authentic audio evidence being misclassified as deepfakes) and false negatives (i.e., deepfakes not being identified as such) each pose different types of risks to the administration of justice. False positives can lead to the exclusion of relevant evidence, whereas false negatives can result in the admission of fabricated evidence. Therefore, courts must develop protocols that acknowledge these risks and assign the burden of proof accordingly.[1017]

ETHICAL CONSIDERATIONS AND SAFEGUARDS

- **Safeguarding Legitimate Uses of Voice Synthesis**

Any regulatory regime must also provide for safeguarding legitimate uses of voice synthesis:
1. Satire and parody
2. Educational demonstrations
3. Accessibility tools for individuals with speech disabilities
4. Entertainment and media productions

Therefore, India's regulatory regime must adopt a constitutional approach that views the risks posed by deepfakes as new challenges based on new technologies, but not new constitutional challenges. Therefore, regulation of deepfakes must rely "on a strong expansion of existing legal doctrines, with suitable safeguards for satire, parody, and artistic freedom".[1018]

- **Preventing Misuse of Detection Technologies**

Detection technologies could be weaponized –

[1014] Beaver. (2025). Budapest Convention and deepfake gaps: Cross-border investigation protocols. Journal of Cybercrime & Digital Evidence, 14(2), 145–168
[1015] Chandrapalan. (2025). Adversarial robustness challenges in deepfake detection systems. International Journal of Artificial Intelligence Security, 9(1), 33–59
[1016] Sharma, P., et al. (2025). The technological arms race: Adversarial robustness challenges in deepfake detection. Pattern Recognition Letters, 185, 35–52
[1017] Rodgers, J., et al. (2024). Forensic audio professionals' ability to distinguish authentic from synthetic voice samples: False positive risks and the "Liars Dividend." Science & Justice, 64(5), 402–417
[1018] Kumar, R. (2025). Synthetic voice impersonation technology and the "Liars Dividend": Regulatory gaps and comparative legal safeguards. Asian Journal of Law and Technology, 11(2), 177–210

e.g., law enforcement could use accusations of deepfakes to target marginalized groups or vulnerable individuals. Therefore, clear and transparent oversight mechanisms must be developed to govern the use of detection technologies and to prevent the misuse of such technologies.[1019]

CONCLUSION

Synthetic voice impersonation represents a new and growing threat to the integrity of the judicial processes in India. Current legal frameworks in India do not adequately address the issue of deepfake audio in judicial proceedings. Although India has made significant advancements in modernizing its evidence laws through the enactment of the Bharatiya Sakshya Adhiniyam, 2023, and refining its criminal laws through the enactment of the Bharatiya Nyaya Sanhita, 2023, there are still no specific provisions in these laws that deal with the authentication of deepfake audio in judicial proceedings.

In particular, the criminal justice system in India relies heavily on the reliability of the evidence presented in court, and audio evidence that is not reliably authenticated undermines the entire premise of the criminal justice system. India's forensic laboratory infrastructure is improving, but it does not currently possess the specialized capabilities to analyze deepfake audio, nor does it have standardized methodologies for analyzing such evidence that are accepted across all forensic science laboratories.

Therefore, key recommendations for India's regulatory response include:

1. Enact specific legislation that criminally addresses synthetic voice impersonation and enhances penalties for judicial misuse of deepfakes;
2. Amend the Bharatiya Sakshya Adhiniyam, 2023 to include provisions that establish standards for authenticating deepfake audio;
3. Strengthen forensic laboratory capacity through the establishment of specialized audio forensic units and international accreditation (ISO 17025) for audio forensic work;
4. Provide judicial training on deepfake technology and the evaluation of such evidence;
5. Create mechanisms for inter-agency coordination between forensic science laboratories, law enforcement agencies and the judiciary;
6. Harmonize international regulatory approaches, while maintaining the constitutional safeguards for legitimate speech and artistic expression;
7. Develop cross-border investigative protocols for transnational deepfake crimes.

The challenge of responding to the problem of deepfakes is multi-faceted — technological, legal, institutional and ethical. A single legislative amendment will not suffice to solve this problem. Rather, India must implement a comprehensive and coordinated policy response that incorporates legal reform with the development of forensic laboratory infrastructure, institutional capacity building, and ongoing international engagement. Only by implementing such a comprehensive strategy can India protect the integrity of its judicial system, preserve the rule of law, and protect the fundamental rights of its citizens in the digital age.

REFERENCES

Beaver. (2025). Budapest Convention and Deepfake Gaps; Cross-Border Investigation Protocols.

Chandrapalan. (2025). Adversarial robustness challenges in deepfake detection systems.

Deshpande, et al. (2025). Machine learning-based classification models for deepfake audio detection with CNN-BiLSTM architecture.

Goyal, & Mali. (2025). Evidentiary challenges in Indian courts; integration with digital evidence frameworks; cross-border digital evidence challenges; voice data protection implications.

[1019] Singh, A., et al. (2025). Electronic records authentication under the Bharatiya Sakshya Adhiniyam, 2023: Evidentiary standards for audio evidence. Journal of Indian Law and Society, 16(1), 91–118

Gunzo, et al. (2025). Multi-factor verification systems combining voice biometrics with facial micro-motion analysis and liveness detection.

Khokhlova. (2025). Criminal implications of synthetic voice impersonation through deepfake technology.

Kishwar, et al. (2025). Digital Personal Data Protection Act, 2023 and voice biometric data protection.

Kothari, & Tibrewala. (2024). Synthetic voice impersonation as a threat to judicial integrity and fair trial rights; evidence tampering and chain of custody issues.

Kumar. (2025). Definition and evolution of synthetic voice impersonation technology; threats to judicial integrity; the "Liars Dividend" concept; regulatory gaps in Indian legislation; comparative legal approaches; and safeguards for satire and artistic freedom.

Mosechkin. (2025). Russian criminal jurisprudence precedents on falsification of biometric data through AI systems.

Ouahab, et al. (2024). Voice biometric technology as evidence in legal proceedings.

Pathak, et al. (2025). Informed consent in voice authentication and voice data disclosure.

Rodgers, et al. (2024). Forensic audio professionals' ability to distinguish authentic from synthetic voice samples; false positive rates and the "Liars Dividend."

Sayyed. (2024). Criminal offenses facilitated by synthetic voice impersonation; attribution of criminal responsibility in AI-generated content.

Sharma, et al. (2025). Adversarial robustness challenges and technological arms race in deepfake detection.

Singh, et al. (2025). Bharatiya Sakshya Adhiniyam, 2023 provisions for electronic records authentication; evidentiary standards for audio evidence.

Singh. (2023). Forensic infrastructure limitations in India; deepfake audio detection capabilities; chain-of-custody practices; institutional expansion and standardization requirements.

Smanova, et al. (2025). Vulnerability of voice biometrics to deepfake attacks and authentication reliability.

Srinagesh. (2024). Technological detection methods using spectro-temporal analysis with CNNs and RNNs.

Williams, et al. (2025). Detection methods focusing on harmonic structures and formant patterns in synthetic voice identification.

Wu. (2025). Deep learning models (WaveNet and Tacotron) for synthetic voice creation replicating vocal characteristics.