
AI VOICE CLONING FRAUDS: EMERGING CHALLENGES FOR INDIAN CRIMINAL LAW

Dr. Neeraj Jain, Assistant Professor, Department of Law, Chaudhary Ranbir Singh
University, Jind, (Haryana)¹

ABSTRACT

Artificial intelligence (AI) has revolutionized communication technology by providing a platform to machines to produce extremely lifelike synthetic voices that can replicate voice, tone, accent and speech of people in an impressive manner. Although voice cloning technology is being used by many useful purposes such as service for disabled, entertainment, customer support and digital communication, wrong use of this technology has led to emergence of whole new category of cyber-enabled offenses. AI voice cloning has become an effective method used by offenders in their activities such as impersonation, scamming, identity theft, extortion, disinformation campaign and manipulation of digital evidence. The development of voice-based digital payment systems, online banking and voice authentication system in India has made citizens vulnerable to voice-cloning frauds.

The objective of present paper is to examine emerging issue of voice cloning frauds committed with use of artificial intelligence and analyze adequacy of Indian criminal laws to deal with such violations. This research paper will explore relevance of Bharatiya Nyaya Sanhita, 2023, Information Technology Act, 2000, Bharatiya Sakshya Adhiniyam, 2023 and Digital Personal Data Protection Act, 2023 in dealing with crimes committed with help of voice cloning techniques. The research will also discuss issues related to using evidence obtained from audio files generated with use of artificial intelligence. The paper will refer to recent literature sources covering topic of voice cloning, audio forensics, deepfakes detection and AI-enabled crime to reveal gaps in existing legal regulation of problem under consideration. Thus, while there are certain laws that offer some solution to problem through provisions related to cheating, impersonation, identity theft, forgery and cybercrime, these provisions were not intended for AI-generated synthetic media.

Keywords: Artificial Intelligence, Voice Cloning, Deepfake Audio, Bharatiya Nyaya Sanhita, Cybercrime, Digital Evidence, Audio Forensics, Identity Theft, Criminal Law, AI Governance.

¹ Assistant Professor, Department of Law, Chaudhary Ranbir Singh University, Jind, (Haryana)

Introduction

The tremendous pace at which AI technologies have progressed has led to a revolution in digital world due to ability of machines to imitate human intelligence and communication. Perhaps one of most noteworthy advancements is development of artificial intelligence-based voice cloning technology that allows for production of realistic-sounding speech that mirrors voice traits of an individual. The latest deep learning models are so sophisticated at imitating intonation, accent, emotional expression and speech rhythm that even forensic experts find it increasingly hard to differentiate between real voices and their synthetic clones.²

Voice cloning technology has developed from a niche scientific product into an extensively available commercial good. There are many websites which offer to clone voices by using just several seconds of audio samples to produce realistic artificial voice. Even though such technologies have legal uses in sphere of education, entertainment, accessibility services, customer support and digital media production, they are often misused which results in cybersecurity, privacy and criminal issues.³

One of most dangerous examples of misuse of AI voice cloning technology is use of voice cloning for criminal purposes. Criminals use cloned voices to impersonate relatives, corporate leaders, government officials and representatives of financial organizations. In such cases criminals exploit trust people put in their familiar voices. Unlike regular phishing that works through written communication, voice-cloning phishing scams use psychological tricks and techniques of social engineering to trick people.⁴

Several recent studies prove that artificial voices can deceive not only humans but also voice authentication technologies. Increasing development of deep fake audio technologies made voice recognition based methods of verification obsolete. As a result, industries like banking, digital payments, e-commerce and telecommunications are especially exposed to AI-based impersonation attacks.⁵

However, threat caused by voice cloning is not confined to financial fraud only. Cloned voice

² Hasmita Kaur, "Detection of AI-Generated (Cloned) Voices Using Audio Forensics: A Review" in *Proceedings of First International Conference on Advances in Forensics and Cyber Technologies (ICFACT 2025)* 224.

³ Ibid.

⁴ Ram Pratap Singh, "A Review on Voice-based Scam Detection Using Machine Learning and Speech Analytics" (2026) 3(5) *Journal of Science Engineering Technology and Management Science* 271.

⁵ Ibid.

technology may also be used to forge evidence, manipulate public perception, disseminate misinformation, perform propaganda, carry out blackmailing and subvert course of justice. In fact, very possibility to clone voices in order to record statements which people did not make creates a problem concerning reliability of digital evidence and credibility of voice recordings.⁶

There are many factors that favor use of cloning technology by criminals in India, whose digital environment is growing rapidly. The wide use of Unified Payments Interface (UPI), mobile banking apps, digital wallets and call center technologies opens up new prospects for criminals using AI-generated voice clones. Cases of scams committed via impersonating relatives and bank employees using cloned voices have been reported recently. This fact demonstrates inefficiency of traditional security measures concerning this issue.⁷

This question takes on greater complexity when viewed from perspective of criminal law. Criminal acts such as cheating, personation, forgery, criminal intimidation and identity theft were envisaged at a time when human beings personally committed deceptive activities. AI voice cloning adds another layer of technology which brings challenges in connection with attribution, mens rea, causation and admissibility of evidence. Due to decentralised nature of AI technology, identification of individual behind creation, deployment or distribution of cloned audio becomes exceedingly difficult.⁸

In addition to this, advent of AI voice synthesis is causing problems for laws of evidence. It was traditionally assumed that audio recordings were credible pieces of evidence that could be verified through forensic analysis. But with deepfake audio technologies, assumption of veracity of recorded speeches is now being questioned as courts and investigators must deal with prospect of a recording that can be completely fictitious.⁹

New research on AI-enabled crime highlights voice cloning technology as being part of a much wider phenomenon of “industrialization of deception.” Through AI technology, criminals can achieve automation, scalability and personalization of fraud crimes in a manner never seen before. Generative AI technology cuts down costs and makes deception more efficient, thus

⁶ Paolo Bailo et al., “A Review of Crime at Machine Speed: Criminological Aspects of Artificial Intelligence’s Industrialisation of Deception” (2026) 8 *Sci* 54.

⁷ Ram Pratap Singh, *supra* note 3.

⁸ “When Technology Lies: Deepfake and Criminal Law in India” 4–5.

⁹ *Ibid*.

empowering both organized crime syndicates and individual criminals.¹⁰ The confluence of AI, social engineering and cybercrime constitutes a paradigm shift in nature of criminal activity and not simply a technological change.

Presently, India's legislation deals with AI-based threats using general criminal laws and cybercrime laws. The Bharatiya Nyaya Sanhita, 2023 provides provisions dealing with offenses such as cheating, impersonation, forgery, identity theft and intimidation which may be employed in tackling voice cloning fraud. In addition, Information Technology Act, 2000 has provisions for dealing with offenses such as identity theft, cheating by personation using computer resources and unauthorized access to computing facilities. The Bharatiya Sakshya Adhiniyam, 2023 deals with electronic record admissibility, whereas Digital Personal Data Protection Act, 2023 provides very limited protection for biometric and personal data collection and processing.¹¹

However, despite these provisions, there still exist certain difficulties. The relevant laws were not framed in light of use of AI technology for creating synthetic media. As a result, they tend to need a broad interpretation in order to cover criminally innovative behavior. Moreover, problems connected with jurisdiction, liability of platforms, algorithmic accountability and forensic authentication remain unaddressed.¹²

This paper tries to address mentioned challenges through a critical analysis of technology used in AI voice cloning, criminology of voice frauds and applicability of modern Indian criminal law to offenses with respect to synthetic audio. The aim of this paper is to analyze whether modern legal framework can be considered appropriate enough in order to deal with challenge posed by AI voice cloning.

Evolution of AI Voice Cloning Technology and Emerging Criminal Risks

Voice Cloning is term used to refer to process through which artificial intelligence generates speech that mimics vocal qualities of target speaker. In modern voice cloning techniques, artificial intelligence systems mainly use deep neural networks, machine learning algorithms and text-to-speech architectures that can learn complex acoustic patterns from recordings of

¹⁰ Paolo Bailo et al., *supra* note 5.

¹¹ Bharatiya Nyaya Sanhita, 2023; Information Technology Act, 2000; Bharatiya Sakshya Adhiniyam, 2023; Digital Personal Data Protection Act, 2023.

¹² "When Technology Lies: Deepfake and Criminal Law in India", *supra* note 7.

human speech. Voice cloning models today can mimic linguistic subtleties, emotions and voices with remarkable accuracy, making it impossible to distinguish between synthetic and natural speech under normal circumstances.¹³

Previous speech synthesis models generated computerized and easily recognizable sounds. However, with advancements in deep learning models, voice synthesis has become much more realistic. Techniques like neural text-to-speech, voice conversion model and generative adversarial networks make it possible to produce very realistic synthetic voices with just little source data. Some voice cloning models work with just a couple of seconds of recorded voice to produce realistic voice copies.¹⁴

Ease of access to such technologies has also led to their abuse. Commercial voice cloning platforms abound and do not require any special technical skills on part of user. The advent of democratized AI has allowed cybercriminals to harness power of AI and engage in malicious activities using voice technology. Whereas in past voice cloning could only be done in sophisticated laboratories, nowadays everyone with access to Internet can make use of it.¹⁵

Perhaps most common form of AI-enabled voice fraud is voice phishing or vishing. Offenders engage in voice-cloning to pretend to be another person and obtain certain information or authorization for carrying out certain transactions or manipulate victim into transferring money. As opposed to conventional phishing, voice-cloning allows exploiting emotions of trust and social familiarity, thus making detection of such crimes rather difficult.¹⁶

Another type of fraud is an executive impersonation scam. Offenders create voice clones of executives of a company and give instructions to its employees regarding financial transactions or transfer of certain information. Several cases that occurred internationally have proven how effective this scheme is and have resulted in great financial damage for organizations.¹⁷

The rise in realism of AI voice generation technologies also raises concerns about its implications for law enforcement and judiciary. Audio recordings have long played an important role in criminal investigation practices. In this context, however, prevalence of

¹³ Hasmita Kaur, *supra* note 1.

¹⁴ *Ibid.*

¹⁵ Paolo Bailo et al., *supra* note 5.

¹⁶ Ram Pratap Singh, *supra* note 3.

¹⁷ *Ibid.*

deepfake technologies raises questions regarding ability to rely on such evidence as a sign of veracity. In face of constantly improving synthetic audio generation technologies, forensic experts become unable to distinguish real recordings from manipulated ones.¹⁸

In response, new methods for forensic audio analysis are introduced. In conventional forensics, acoustic analysis, spectrographic analysis and speaker comparison were used. Recently, machine learning-based detection of anomalies in synthetic speech is becoming increasingly popular. However, arms race between detection tools and voice generation technologies persists.¹⁹

Misuse of voice-cloning technology illustrates way this problem goes far beyond technological advancement. With increasing spread of AI voice deception, new problems arise in terms of criminal law and digital governance.

Applicability of Indian Criminal Law to AI Voice-Cloning Frauds

The problem created by advancement of artificial intelligence in creating voice clones is a great challenge to criminal law in terms of deception through creation of a false identity and not through direct human impersonation. Nonetheless, there are provisions contained in Bharatiya Nyaya Sanhita, 2023 (BNS) and Information Technology Act, 2000 that could be used to charge persons committing crimes using voice clones.

Cheating is one of offences provided for under BNS and which can easily apply to voice-cloning cheats. Cheating, which involves deceiving people in order to make them suffer wrongful loss through giving up money or making them do something or giving out confidential information, is applicable in voice-cloning cases where a person uses voice clones to pretend to be their family member, boss, bank or government officer and thus makes them send money.²⁰

Offences related to personation take on fresh importance in light of voice-cloned speech generated by AI. While act of personation traditionally involves representing oneself as another in physical form, with advent of voice cloning, personation is now possible digitally. The offender need not resemble person in terms of physical likeness; it is sufficient for voice to be

¹⁸ Hasmita Kaur, *supra* note 1.

¹⁹ *Ibid.*

²⁰ Bharatiya Nyaya Sanhita, 2023, provisions relating to cheating and dishonest inducement.

a clone. In such circumstances, provisions related to cheating by personation will apply to cases involving voice-cloning fraud.²¹

Moreover, there are many provisions within Information Technology Act, 2000 that can be used to counter voice-cloned fraud. These include provisions related to identity theft and cheating by personation by using computer systems, which are relevant since voice cloning requires computers in order to produce, store and transmit speech data. If offenders use voice cloning to gain unauthorized access to bank accounts, digital wallets or any other confidential information, they would be liable for cyber crime as well as general criminal laws.²²

A further problem occurs where AI-produced voices are used to produce fake audio recordings. Such fake audio recordings can be used for purposes such as manufacturing of false evidence, tarnishing of reputations, blackmailing people and manipulation of public sentiment. In such cases, laws dealing with forgery or fabrication of evidence are applicable. While traditional ideas of forgery are concerned with physical documents, modern day notions of forgery have evolved to take into consideration electronic records as well. Thus, an audio recording that is produced using artificial intelligence and which has ability to deceive listeners about its genuineness can be considered digital forgery that needs criminal liability.²³

Misuse of synthetic voices could be considered criminal intimidation, extortion or defamation depending on content of communication. Offenders use artificial voices to threaten victims, make false allegations and fabricate confessions among others.²⁴

Nevertheless, while there are such options for regulation available, there is still an issue of legal doctrine that needs to be tackled. The existing offences are not specifically tailored for any kind of artificial intelligence technologies. As a result, courts need to conduct an expansive interpretation and apply general legal notions to technologically new types of misbehaviour, which introduces some uncertainties into question of what actions will lead to criminal responsibility.²⁵

The same applies to attribution. Fraudulent practices involving voice cloning require

²¹ Information Technology Act, 2000, provisions relating to cheating by personation using computer resources.

²² Information Technology Act, 2000, ss. 66C and 66D.

²³ “When Technology Lies: Deepfake and Criminal Law in India” 8–10.

²⁴ Ibid.

²⁵ Ibid.

cooperation of several people from different jurisdictions. Someone collects audio clips, someone trains artificial intelligence to recognise certain sounds, someone creates voice imitations using collected material and someone distributes audio. It makes determining who actually had a guilty mind and therefore deserves to be punished much more complicated than in ordinary fraudulent schemes.²⁶

At same time, this task becomes even harder due to increasing accessibility of artificial intelligence technology. Now people do not need advanced knowledge to create quite convincing fake voices because everything needed is freely available online. Therefore, it becomes difficult for police to track down sources of any manipulated audio and find out who created it.²⁷

Evidentiary Challenges under Bharatiya Sakshya Adhiniyam, 2023

Undoubtedly, one of greatest challenges raised against voice-cloning technology from a legal perspective arises out of law of evidence. Historically, audio recordings have been considered valuable sources of electronic evidence, which can help confirm witness accounts and establish facts and intent. The courts have proceeded under assumption that recording was a product of human interaction until manipulated evidence has been proved.²⁸

In accordance with provisions of Bharatiya Sakshya Adhiniyam, 2023, electronic records can be treated as admissible evidence under certain circumstances. The statute itself operates on assumption that electronic record can be authenticated through technical certification and verification procedures. The issue with deepfake audio technology is that audio record can be generated without leaving any evident marks of manipulation.²⁹

The rise of what scholars refer to as "deepfake defence" demonstrates this point. In criminal cases, defendants may raise their defences arguing that genuine recordings of their voice are not genuine but are artificial products of AI. Alternatively, fake recordings can be admitted into evidence as true recordings. In both cases, court will have to distinguish real from

²⁶ Ibid.

²⁷ Paolo Bailo et al., *supra* note 5.

²⁸ Andrea Roth, "Machine Testimony" (2017) 126 Yale Law Journal 1972, discussed in "When Technology Lies: Deepfake and Criminal Law in India".

²⁹ Bharatiya Sakshya Adhiniyam, 2023.

technologically generated deception.³⁰

Traditionally, forensic techniques involve acoustic examination, spectrographic analysis, waveform comparisons and speaker recognition approaches. Although these forensic techniques continue to prove useful, studies suggest that sophisticated voice cloning systems are becoming progressively adept at fooling conventional forensic systems.³¹

Consequently, researchers have introduced new forensic systems based on machine learning that detect minute artefacts in voice produced by artificial intelligence. The detection process involves analysing patterns associated with frequency distribution, prosody, temporal regularity and spectral distortions. Despite these developments, current detection technologies continue to suffer from flaws since criminals keep modifying their approach to circumvent forensics.³²

There is an obvious implication for criminal justice in all this. Should courts no longer be able to place full reliance on recorded speech as proof of actual events, entire process of investigation and prosecution will face challenges. This means that criminal justice institutions will need to establish standards for authentication of AI-sensitive evidence. Such standards may include mandatory forensic evaluation, requirement of expert testimony, digital provenance and even blockchain-based evidentiary protocols.³³

Need for Regulatory Reform and Future Directions

Analysis performed in this paper shows that AI-based voice-cloning frauds are more than a typical cybercrime issue. AI voice-cloning crimes pose structural problems for legal systems by undermining trust in identification, communication and evidentiary processes. Current Indian regulations include certain legal instruments in form of provisions on cheating, personation, identity theft, forgery and cybercrime that can partly serve as an answer to AI voice-cloning cases. Yet, current provisions are reactive instead of preventive and are not developed specifically for cases of AI voice-cloning.³⁴

First of all, law should introduce definition of synthetic media and AI-generated impersonation,

³⁰ “When Technology Lies: Deepfake and Criminal Law in India”, supra note 7.

³¹ Hasmita Kaur, supra note 1.

³² Ibid.

³³ Ibid.

³⁴ Paolo Bailo et al., supra note 5.

which would resolve issues of uncertainty about application of criminal offences to voice-cloning cases. Legal provisions should be introduced that criminalise malicious creation, dissemination and employment of synthetic voices with purpose to deceive, defraud, intimidate or manipulate people.³⁵

Secondly, India needs to introduce special legislation governing harvesting and utilization of biometric voice data. Although Digital Personal Data Protection Act, 2023 already serves as basis for such regulation, it does not provide specific rules related to AI voice cloning. It is important to improve existing regulations concerning use and harvesting of voice data.³⁶

Third, law enforcement needs technological capacity building. Proper investigation of use of AI technologies in criminal offences requires having specialized forensic labs, digital forensics experts and necessary equipment. Therefore, there is a need for investing in audio forensic technology capabilities.³⁷

Fourth, internet platforms and AI technology companies need to take up more responsibility in curbing misuse. Regulations should make them accountable for transparency, labeling of content, risk assessments and removal of harmful synthetic audio content. This would bring India in line with global trends in regulation of AI technology and internet platforms.³⁸

Fifth, courts need to establish solid rules on how to deal with synthetic audio in evidence matters. Proper judicial training and AI-related expert witnesses would be key in sustaining trust in electronic evidence in legal process.³⁹

Conclusion

In addition to providing new possibilities for innovation, Artificial Intelligence has opened doors for criminals. One such technology is voice-cloning technology. It has been used by offenders not only in order to create useful products but also as an efficient tool of committing frauds, impersonations, identity theft, spreading misinformation and manipulating evidence.

It is shown that voice-cloning technology raises serious legal problems in Indian criminal law

³⁵ Ibid.

³⁶ Digital Personal Data Protection Act, 2023.

³⁷ Hasmita Kaur, *supra* note 1.

³⁸ Paolo Bailo et al., *supra* note 5; Artificial Intelligence Act, Regulation (EU) 2024/1689.

³⁹ “When Technology Lies: Deepfake and Criminal Law in India”, *supra* note 7.

due to its disruption of traditional assumptions about identity, communication and authenticity. Legal tools to prevent such behavior include provisions contained in Bharatiya Nyaya Sanhita, 2023, Information Technology Act, 2000, Bharatiya Sakshya Adhiniyam, 2023 and Digital Personal Data Protection Act, 2023. However, these laws were made before emergence of generative AI and thus cannot effectively protect against unique harms posed by synthetic media.

As voice-cloning technology advances, there is a need for preventive measures. The future legislation should include changes to criminal law, data protection laws, forensic developments, platform responsibility and court training. Only then India will be able to cope with frauds committed through AI voice cloning.