WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

AI-Driven Digital Arrest Scams: Legal Gaps in Regulating Deepfake Impersonation

Rishabh Chaudhary [*] ***Dr. Kanika Aggarwal*** [**]

SRM School of Law, SRM University, Sonepat, Haryana, India.

ABSTRACT :

AI-generated digital arrest scams have appeared as a new frontier of cybercrime in India, wherein deepfake technology is exploited to impersonate law enforcement agencies and coercively extort money or data from unsuspecting victims. These scams interfere with the victims' psychological responses by presenting an outside threat in the form of hyper-realistic video or audio impersonation by official authorities, which thus induce fear and urgency. Hence, this paper looks at technological infrastructure behind the making of such scams, mainly the deepfake generation using Generative Adversarial Networks, while also critically explaining India's legal preparedness to counter such offenses. Statutes like the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 contain provisions related to cheating and impersonation. Still, none categorically address synthetic identity manipulation. The study calls out the interpretative gaps and enforcement impediments caused by archaic legal language, lack of evidentiary procedures, and cross-border jurisdictional constraints. It places emphasis on the analysis of real-world cases and judicial responses to bring forth the challenges in the existing legal remedies, particularly in proving AI-mediated fraud and preservation of admissible digital evidence. The findings call for a multipronged legal reform that contemplates statutory recognition for deepfake impersonation, judicial training, forensic modernization, and cross-border cooperation. It also calls for regulatory measures with the power to penalize malicious synthetic identity generation without hampering lawful applications of AI. The menace of uncontrolled abuse of AI is not a personal complaint but more than a dent to the credibility of e-governance and to the confidence reposed by citizens in digital institutions. Thus, the time is ripe for a clear-sighted, pro-active legal-policy response to overcome this newly sprung and rapidly changing cyber challenge.

Keywords: Deepfake Impersonation, Digital Arrest Scams, AI-Generated Fraud, Information Technology Act, Bharatiya Nyaya Sanhita, Cybercrime Law, Synthetic Media Regulation, Digital Evidence Authentication.

Introduction

With the advancement of AI tools over the years, the channels through which criminal activities are carried out over digital platforms have undergone radical changes. A recent spate of AI-based digital arrest scams has been recently seen in India. The scams are sophisticated in nature and make use of AI-created deepfake content to build a believable replica of law enforcement authorities or government officials. The impostors then trick victims into thinking that they are targets of legal inquiries or arrest warrants and forcing them to pay or provide personal details. These frauds are both economically and psychologically crippling, depriving the citizens of the trust to use digital communication platforms and public organizations. The present study would shed light on such a disturbing upsurge of such scams, with an attempt to gauge how deepfake technology enhances their impact and determine vital lacunae in the Indian legal structure through which such fraud thrives. By the analysis of the existing statutory instruments and tools to impose them, the study aims to assist further debate on the regulation of digital impersonation by AI and propose potential lines for policy and legislation.[1]

Definition and Explanation of AI-Driven Digital Arrest Scams

One-ever-increasing field of AI device sophistication has revolutionized criminal activity on digital platforms. The recent past in India has witnessed a rise in cybercrimes driven by AI- AI-Driven Digital Arrest Scams. In this sophisticated crime, the perpetrators use AI-created deepfake media to pose as law enforcement or top government officials. The victims are made to believe that they are targets of some form of legal inquiry or warrant of arrest and are subsequently either threatened into making some sort of payment or releasing some sort of personal data. The severity of these scams is not merely financial but also psychological, as they erode people's trust in digital platforms of communication and public institutions. This study puts into the limelight the somber rise of these frauds, evaluates the manner in which deepfake technology amplifies their impact, and identifies key gaps in the Indian

[*] Student, LL.M. (Master of Laws), SRM School of Law, SRM University, Sonepat, Haryana, India.

[**] Assistant Professor, SRM School of Law, SRM University, Sonepat, Haryana, India.

[1] Online Bureau, "Rising threat of 'Digital Arrest' exploiting deepfake sparks concern among law enforcement", *available at:* https://legal.economictimes.indiatimes.com/news/law-policy/rising-threat-of-digital-arrest-exploiting-deepfake-sparks-concern-among-law-enforcement/114274182 (Visited on March 7, 2025).

legal system that enable such frauds to persist. This study aims to maintain debate on regulating AI-driven online impersonation and propose viable legislative and policy solutions by analyzing existing statutory provision and enforcement mechanisms.

Importance and Relevance of the Topic

With the immediate legal and academic attention that this matter demands, it is clear that AI-driven digital arrest scams have had a much-touted impact on Indian society, with this impact increasing continuously across a vertical. It is in India that the digital black hatters might truly prosper-the land of 750 million-plus internet users as of 2024. Recent statistics revealed that losses in terms of finances exceeded ₹120.3 crore just in the first quarter of 2024 from digital arrest scams. The money was a trifle; let's look at the psychological trauma: one remembers the continuing tales of anguish from victims-a Type A! Lullabies of panic, all-nighters, climaxes of feeling scorned, betrayed, and ashamed. The trust in digital platforms as applicable media for official communication has been badly eroded. When the everyday man starts doubting if this very video call from the police or a text from a government helpline is an authentic one, then obliviously lying at the doorstep are grave consequences on the very genuine processes of law enforcement. The credibility of digital governance, which is at the heart of programs such as "Digital India" and digitization of legal and administrative services, also comes under great stress. There rise questions of a broader nature about whether existing legislative tools is adequate enough to face the challenge. Laws such as the "Information Technology Act, 2000", although at the time of their enactment were up to date and broad in scope, would, however, not envisage a situation where AI-based manipulations were concerned. All these developments draw attention to the immediate need for amendment or supplementation of existing legislation to counter the convoluted and adaptive threats of AI-based digital fraud. It is hence a challenge to address this case by a multidimensional legal doctrine, which considers psychological, technical, and regulatory issues.[2]

Research Objectives

AI-driven digital arrest scams deserve immediate intervention, both legal and academic, for the immense and growing impact on Indian society. As digital penetration is ever-increasing-statistics speak of over 750 million internet users in India as of 2024-the country stands well-placed for digital exploitation. Recent data reveals that financial losses through digital arrest scams reached over ₹120.3 crore in the first quarter of 2024 alone. However, the amount of money involved is merely the tip of the iceberg. Many victims speak of long-term psychological agony, such as anxiety, disturbed sleep patterns, and a profound feeling of betrayal and shame. Trust in digital media as a safe platform for official communication has severely eroded. The moment people start wondering whether a video call from a police officer or a text from a government helpline is fake, the damage begins to creep into the veracity of real-world law enforcement processes. Digital governance, which is so centrally tied with the "Digital India" program and digitization of legal and administrative services, gets greatly undermined because of this. Thus, the rise of these scams opens up wider questions on the adequacy of our current legislative tools. When the Information Technology Act of 2000 was enacted, it was a comprehensive legislation that could not foresee the phenomenon of AI-generated manipulations. These developments emphasize the need to amend or supplement laws in order to equitably address the multifarious, shifting threat posed by AI-facilitated digital frauds. Now to tackle this, there must be a multidimensional approach towards the legal strategy that looks at the psychological, technical, and regulatory intricacies simultaneously.[3]

Understanding Deepfake Technology

The essence of the AI-powered digital arrest scam continues to lie in the sophisticated multimedia manipulation of deepfake technology. With the advent of changing intricacies casted on digital platforms, AI-facilitated perpetrators not only mimic the human behavior and appearance with very high resolution but also emulate it. Such representations of deepfake technology are calibrated to deceive the victims into accepting false fabricated communications, ranging from impersonating officials to law enforcement agents. To realize how this technology supports the execution of digital arrest scams, one will need to analyze deepfakes in their essence, the methodology of their creation, and how the essence of AI developments allowed deepfakes to advance to more realistic ones and become more easily available.

What Is a Deepfake?

The concept itself of digital arrest scams is based on the use of deepfake technology with evil undertones in terms of multimedia manipulation. The more sophisticated digital ecosystems seem, the more susceptible they are to be exploited by malpractitioners using artificial intelligence not only for simulating but for exactly copying human behavior and likeness. Equipped with deepfake technology, fraudsters produce information that is capable of mimicking the voice and image of real individuals, including government representatives and law enforcement officials. This manipulation makes fraudulent communications more believable and harder to track. To grasp how this technology is used to commit digital arrest scams, one must first gain an understanding of the nature of deepfakes, the methods through which they are produced, and how recent advances in AI allow them to become more realistic and attainable.[4]

---

[2] Legal Challenges of Deepfake Technology and AI-Generated Content in India, *available at:* https://www.juscorpus.com/legal-challenges-of-deepfake-technology-and-ai-generated-content-in-india/ (Visited on March 21, 2025).

[3] Ajuni Bedi, "Legal Challenges in Regulating Deepfake Technology: Key Issues & Future Implications", *available at:* https://lawchakra.in/blog/legal-challenges-deepfake-technology/ (Visited on April 6, 2025).

[4] Shinu Vig, "Regulating Deepfakes: An Indian perspective", 17 *JSS* 70 (2024).

How Deepfakes Are Created

Deepfakes are those images, videos, and audio recordings made using computers that may show a real event or an invention of one, depending on the motivation of the creators. This manipulation makes these digital doppelgangers nearly impossible to distinguish from genuine recordings in one's perspective creating such a strong delusion of authenticity. On the harmless end, deepfakes might attempt to duplicate scenes for motion pictures, recreate old footage, or make realistic digital avatars in gaming. On the drastically other end, malicious deepfakes are found to impersonate a public figure for the spreading of disinformation and perhaps the most important issue of defrauding by mimicking the identity of some legitimate authority. For example, an impersonation of a fake police official issuing threats over a video call for arrest may look quite convincing-especially when the visuals of the official's uniform, facial expressions, and speech patterns have all been digitally attained to perfection. The very success of these impersonations lies in the human nature to trust visual and auditory cues which officially corroborate with the established authorities. In these digital arrest threats scams, a digital rendition of a police officer or bureaucrat speaking in the vernacular and referring to authentic-sounding sections of law imparts highly convincing deceit. This reason not only distorts the content of communication but equally distorts the medium of transmission and thus becomes a very powerful tool of AI-based forgery.

The Role of AI in Deepfake Creation

By design, artificial intelligence is primarily intended to create deepfakes; however, it is also the principal force to make a synthetic media artifact more realistic, scalable, and widespread. Over the last decade, especially with innovations in neural networks, natural language processing, and facial recognition systems, deepfakes have had a massive scale improvement in quality and believability. From high-definition facial mapping to automated lip-syncing and proper voice cloning, generated content can now imitate genuine speech or body language with eerie precision. Even more important are the advances in AI that now require far less training data than before to be able to achieve efficiency. Earlier, deepfakes required thousands of photos to be able to REALLY deepfake an output; today's methods seek fewer input modalities for the algorithms to produce plausible outputs, where in some cases, synthesis from an audio recording alone can suffice. One may very well say that the deepfake world is now easy to enter for every creator and distributor. Further, new interfaces provide template-based and automated workflows for non-technical users to manufacture deepfakes. These interfaces, often pitched as entertainment apps or parody tools, can very well be used for malicious intent with no definitive trace. However, the intrusion of those tools into public domains is mostly risking an opportunity for exploitation by fraudsters, as seen in the so-called AI-drive digital arrest scams. Therefore, when AI grants a layperson the power to develop fraudulent content that simulates an authoritative entity, the dispute transcends its technological essence and lands itself squarely on the legal and ethical front. Since the rapid evolution of these tools, any legal system attempting to settle these matters suffers in India because the extant legal framework hardly helps define, regulate, or even detect the very AI-generated impersonations used for crimes. Thus, the penal code's off-the-shelf provisions make it all the more difficult to prosecute an offender, thereby allowing the perpetrators to act with especially bold impunity. Such centrality of AI in greatly expanding the scope of deepfake threats should now lure fancy and action from lawmakers, enforcers, and digital governance bodies.[5]

The Phenomenon of Digital Arrest Scams in India

The advent of AI-powered cyber scams has been causing widespread anxiety among the country's legal, technological, and administrative circles. Digital arrest frauds are among the most devious forms of this phenomenon. The frauds employ a mix of impersonation and deepfake tools targeted towards individuals across socio-economic groups through the mimicking of official communication, making threats, and enforcing compliance on the victim. While scams have in the past involved generic messages or e-mail phishing, digital arrest scams are presented in a far more believable form using personalized video calls, voice synthesis, and forged visual images to masquerade as higher officials. The feeling of deception has been heightened further with the way in which AI technology enables rendering of individuals' images and voices in a seemingly credible manner. Their effectiveness is not only the deception but instilling fear, urgency, and compliance to assumed legal force by filling the human mind. In a legal system itself still working through outdated definitions of technology and sparse provisions relating to AI-based impersonation, online arrest scams become an enigma in regulation as well as enforcement. Addressing them, thus, requires a dive into their modus operandi, their emergence, and the disastrous consequences that have been exhibited in actual cases.[6]

Overview of Digital Arrest Scams

Usually, digital arrest scams commence by means of impersonation, where the miscreants identify themselves as representatives of law enforcement, courts, or regulatory bodies such as the CBI, NCB, or Income Tax Department. The imposter attempts to carry out the act through video call. Through rebuttal, the imposter either claims to possess an official badge, stands in front of a convincing backdrop, or shows orders from a "court" for the imposition of arrest for some offenses or warrants of arrests to individuals. However, such digital evidence does not remain as still images; rather, the imposters put out interactive visuals wherein the 'officer' converses in regional languages, citing real laws like "Section 318 of Bharatiya Nyaya Sanhita" or more famously, "Prevention of Money Laundering Act, 2002", to uphold credibility. With the integration of deepfakes into such scams, the ordinary social engineering is put to shame. No longer is it about guessing a password or hacking an email; it is about manufacture trust by creating a visual and vocal presence that mimics authority figures with an uncanny precision. The targets, often elderly citizens, women living alone, or blue-chip company

[5] F. Muhly, E. Chizzonic, et.al., "AI-deepfake scams and the importance of a holistic communication security strategy", 6 *ICLR* 53 (2025).

[6] Record Of Law, "Deepfake: Unveiling a New Frontier in Cybercrime", *available at:* https://recordoflaw.in/deepfake-unveiling-a-new-frontier-in-cybercrime/ (Visited on April 25, 2025).

employees with little idea of police procedures, are convinced that they are already being watched or under threat from some legal force, hence they must cooperate at once or face arrest, imprisonment, or confiscation of their records. This level of impersonation robs not just the individual but also the public of confidence in governmental communications when they are truthful.

Modus Operandi of Scammers

Digital arrest scams in India usually commence with impersonation, with the fraudsters posing as officials of law enforcement, the courts, or regulatory bodies like the CBI, NCB, or the Income Tax Department. Impersonation occurs in the form of another type of video call wherein, through deepfake technology, the scammer would appear to be a bona fide official bearing forged badges, an official backdrop, and even fake court orders or arrest warrants. These digital elements are not stationary images; these include dynamic, interactive content, wherein the so-called officer converses in the regional language and refers to genuine laws such as "Section 318 of the Bharatiya Nyaya Sanhita", the "Prevention of Money Laundering Act, 2002", and so forth to ameliorate credibility. The incorporation of deepfakes elevates these scams above an average run-of-the-mill social-engineering scam It is no longer just a matter of guessing a password or hacking an email; it is about manufacturing trust-building visual and vocal presence that mimics authority figures with uncanny precision. The targets, often the elderly, ladies living alone, or professionals who do not know police procedures, are led to believe they are being surveilled for a legal threat and have been told to cooperate forthwith to avoid arrest, imprisonment, or asset confiscation. Such impersonation brings individual autonomy into disrepute, along with reducing public faith in legitimate communication from the government.[7]

Statistics and Trends

The method of fraudsters is operationally evolutionary; their modus operandi in cases of arrest is both predictable and very effective. The initial point is usually an unsolicited phone call or message sending a message from a helpline or even a police station. However, the number is usually spoofed on the victim's caller ID to appear from an official source. The moment contact is established, the victim is informed that their name has been linked up with serious criminal charges such as drugs trafficking, financial terrorism, or contravention of foreign exchange regulations. It becomes a fabricated investigation of inter-state or international parcel seizures or some forged biometric data trails so as to free the victim of his wits. Hence, at this stage, there is digital manipulation involved where the scammer initiates a video call: somebody seated in a police uniform in a digitally created police station reading forged official files. The detail in the video surpasses expectations, from fake IDs to seals and signatures convincing enough to make one believe it to be true. Next up are digitally manipulated documents showing the victim's name and photo. Then, in order to avoid immediate arrest, they get coerced into transferring money to "secure bail", pay a "compliance bond", or prove innocence by supplying banking details. Psychological manipulation plays a central role: the scammers instill fear through loud threats but create a pseudo-urgency, telling victims there is "limited time" to respond. They use the trust put on authorities, given how ill-equipped most citizens are in knowing legal procedures by heart and therefore take appearance for authenticity. The success of such techniques lies exactly in the mixture between visible deception and emotional blackmail, which delineates an unprepared witness unless aware beforehand.[8]

Real-life Cases

Coming to the grim scenario of digital scams in India, post COVID, everything went digital, so the trend of scams rose sharply. Official estimates put the amount lost to such scams at ₹120.3 crore for just the first quarter of 2024, indicating an exponential increase in incidents and their monetary amount. More than 6,000 complaints have been recorded all over the country this year, pointing to an unnatural surge, not only in terms of volume but in terms of geographical scope as well-from metropolitan cities such as Mumbai and Bengaluru to semi-urban and even rural areas. Some of these involve victimization cases in which victims were asked to make several payments-ranging from lakhs to even crores of rupees. In tandem with that, banking frauds have increased by 27% in 2024-25 and largely because of AI mechanisms being utilized for impersonation. Deepfake tools have empowered people to become perpetrators of such crimes. Before, there was some technical difficulty that blocked anyone from committing a fraud, but with these freely available software applications, even an amateur can make some very good deepfake videos. This, compounded with data breaches and the availability of personal information online, has given fertile ground for the multiplication of such scams. Law enforcement agencies are overwhelmed by these, lacking forensic tools and statutory backing to effectively respond. Also, sections like "Section 66D of the Information Technology Act, 2000", which penalizes impersonation by means of electronic communication, do not factor in the distinct nature and psychological intensity of AI deepfakes. Redeployment of these legal instruments to combat the technological threats is at the heart of this emerging cybercrime wave.

Legal Framework in India for Cyber Frauds

Some high-profile incidents across India have highlighted the scale and complexity of digital arrest scams by deepfake impersonation. Between 2024 and 2025, Mumbai witnessed the scam where an 86-year-old woman was conned of a whopping ₹20.25 crore by fraudsters posing as police officers investigating financial fraud. These scammers used deepfake video calls and fake digital letters purportedly from banks and government agencies. At one stage, they went further to simulate a court hearing to add credibility to their story. Terrified about any legal consequences, the old lady got fleeced after making multiple transfers for several weeks. A counterpart incident in Kerala had a gentleman aged 73 lose ₹40,000 after someone who looked very much like a deepfake of a colleague had video-called him asking for urgent financial help. The deepfake was so convincing there was nothing to convince the victim otherwise. Another case happened in 2024 in Bengaluru, wherein a group of residents lost ₹95 lakh after being shown deepfake videos having

[7] MP. Sandoval, M. de Almeida Vau, et.al., "Threat of deepfakes to the criminal justice system: a systematic review", 13 *CS* 41 (2024).

[8] Leo S.F. Lin, "Examining the Role of Deepfake Technology in Organized Fraud: Legal, Security, and Governance Challenges", 4 *FIL* 6 (2025).

renowned businessmen like Narayana Murthy and Mukesh Ambani fraudulently endorsing an investment scheme. The cases demonstrated that deepfake impersonations extended outside law enforcement and public figures and that the speed with which such content spread through digital networks only amplified their damage. The hybridity of its technology, emotional appeal, and legal ambiguity has made the incidents very hard to prosecute, and often, with no success. Victims find it hard convincing the police that it really was a scam, while law enforcement agencies appear to lack forensic digital support and jurisdictional clarity. These real-life stories clearly illustrate the pressing need for concrete AI-related legislation and an informed public to combat this new cataclysm.[9]

The Information Technology Act, 2000

In India, the digital revolution has witnessed the rise of cybercrime, particularly those bearing advanced technological methods of perpetration, including AI-enabled and deepfake capabilities. For all instances of such criminal activities, the country principally relies on the Information Technology Act, 2000, which still remains the main legislation concerning illicit activities in cyberspace. Originally aimed at legalizing e-commerce and enabling secure digital interactions, the IT Act has, however, over the years come to be used heavily in a variety of cybercrimes, such as impersonation, unauthorized access, data breaches, and transmission of obscene materials. The adequacy and applicability of this law have been brought under severe scrutiny with the rapid increase in AI-based scams, including digital arrest impersonation scams. The two-fold challenge of law enforcement is; firstly, to somehow graft the existing provisions onto the newer modus operandi of scams and; secondly, to identify gaps of interpretation or procedure that permit the perpetrators to evade liability. While several provisions of the IT Act provide for acts of impersonation, invasion of privacy, and creation and distribution of objectionable material sought to be applicable to acts of objectionable acts of fraud, the same fail to adequately pierce the veil of the complex nature of AI-facilitated fraud, especially when deepfakes come into play to simulate human appearances and speech. The few sections mentioned below shall serve to elucidate the advantages along with some limitations of the present legal landscape to combat these cyber arrest scams.

Section 66D - Cheating by Personation by Using Computer Resource

The "Information Technology Act, 2000" is the main legislation dealing with cyber offenses in India, data protection, and electronic governance. Enacted when digital threats were very elementary in nature, the Act now has several amendments, bringing in various new aspects of identity theft, cyberterrorism, and protection of personal data. The civil and criminal liabilities for offenses committed through the computer system or communication devices are provided for in the framework of this Act. While the Act lays down the basic infrastructure in the form of the "Cyber Appellate Tribunal" and procedure for investigation, it is still challenged by the developing front of AI-based technologies. In particular, deepfake videos and synthetic audio clips used in digital arrest scams present peculiar new challenges that were far from the jurisprudential imagination of the drafters of the Act. Impersonating an authority figure through AI does not simply end up deceiving a victim; rather, it also builds a digital structure in which traditional definition of identity, authentication, and electronic record is not entirely encompassed. The following sections look at how the Act's specific provisions—" Section 66D", "Section 66E", and "Sections 67 to 67B"-are invoked for these kinds of offenses, and if their scope is appropriate for the weight and newness of the deepfake-related scam cases.[10]

Section 66E - Violation of Privacy

This section criminalizes cheating by personation through the use of any communication device or computer resource. How it works is that the Section says that in cases when personation cheats a body by electronic means, the alleged offender shall be punished with imprisonment for a term which may extend to three years and shall also be liable to pay a fine that may extend up to ₹1,00,000. This section is that which comes into play when a fraudster calls pretending to be a bank official, a government employee, or a police officer. Now comes the significance of applying Section 66D in AI-enabled digital arrest scams. These scams purely rely on impersonation, where advanced AI tools like deepfake videos are used to fabricate a visual and audio presence of an official. Victims are forced under the guise of having direct communication with real authorities, making the deception much more convincing and damaging in terms of psychology. However, even though the act of impersonation fits within the terms of the provision, "Section 66D" does not explicitly cater for impersonation that incorporates the fabrication of a person's visual likeness through AI. Its applicability, albeit logical, largely rests upon interpretation, and judicial authorities have to extend the meaning of "impersonation" to cover synthetic identity simulation using AI-generated media. Such an interpretative extension has yet to be fully standardized, leaving a lacuna in both predictability and enforcement. Moreover, the provision does not stipulate higher punishment upon the simulation of legal authority or intimidation upon the victims by fraudulent threats of arrest. Nor does it have any technological specificity willing to identify these unique deepfake tools that do not simply reproduce identity but also emotional cues and behavior.[11]

Sections 67, 67A, 67B - Publishing or Transmitting Obscene or Sexually Explicit *Content*

"Section 66E of the IT Act of 2000" punishes purposely taking, publishing, or transmitting images of a person's private parts without his or her consent under circumstances violating his or her privacy. The Section contemplates a punishment of imprisonment for a term which may extend to three years, or with a fine which may extend to two lakh rupees, or with both. Originally, the section was intended for combating crimes of civil view and covert capture, but some instances may, with limited relevance, apply to deepfakes. Where the generated AI impersonation uses the image of a real person

[9] Kuldeep Singh Panwar, Nilutpal Deb Roy, et.al., "Rising Menace of Deepfakes with the Help of AI: Legal Implications in India", 4 *IJIRL* 94 (2023).
[10] Ganesh Subramanian, Swathi S, et.al., "The Legal Dilemma of Deepfakes AI Liability and the Challenges of Digital Identity Theft", 6 *IJFMR* 1 (2024).
[11] F. Romero Moreno, "Generative AI and deepfakes: a human rights approach to tackling harmful content", 38 *IRLCT* 297 (2024).

without consent, mainly when the victim's face is superimposed onto somebody else's body or placed in videos simulating situations compromising to that individual, the section may be invoked to argue a breach of privacy. On the other hand, the "Section 66E" finds no footing in arrests-by-the-internet scams wherein deepfakes mostly impersonate a third-party official and that too without targeting the victim's image. While the creation without consent of an officer's image might arguably constitute a privacy violation against that officer, it is not contemplated under this provision that impersonation of public figures for the purposes of defrauding a victim is to be treated as a violation of the victim's privacy. However, the issue with applying "Section 66E" in most cases of deepfakes lies in the fact that the latter do not even necessarily feature actual images or video recordings of a person but are rather generated synthetically on the basis of composite data. The absence of an Indian law would further diminish the extent to which "Section 66E" could help curb the creation and dissemination of such synthetic impersonations based on digital likeness. While theoretically applicable where unauthorized use of images occurs, the section lacks clarity or reach to address AI-generated instances of identity manipulation where privacy concerns arise but are implicit and neither compiling nor anatomical.[12]

The Bharatiya Nyaya Sanhita, 2023

"Sections 67, 67A, and 67B" of the Information Technology Act, 2000, attempt to preclude electronic publishing or transmission of any content that is obscene, sexually explicit, or involves children in such explicit manner. Section 67 creates an offence for the publishing or transmission of obscene material; Section 67A deals with sexually explicit acts; and Section 67B deals with child pornography-provided punishments ranging between three and five years of imprisonment and hefty fines. The area most at risk of such application is the misuse of deepfake technology for sexual exploitation, for example, synthetic pornography involving public figures or fabricated revenge material. Although such acts differ from digital arrest scams-notably in that they rarely involve obscene content-this set of laws establishes an important precedent: Indian law will deem synthetically produced media to be a crime if it is obscene or harmful, irrespective of whether it is real or fabricated. Though this recognition is presently not of help in cases where impersonations are used as a tool for legal scams, it certainly opens the door to a rationale that might find similar culpability in cases of AI-based fraudulent impersonation. The drawback is that these provisions address content with obscene and sexual connotations, which is ordinarily absent from digital arrest cases. Hence, while they do show how the law reacts to content-based deepfake abuse, they offer almost no support for victims who face deception or financial coercion through impersonation involving simulated authority instead of obscenity. For the burgeoning class of AI scams using realistic but not obscene deepfakes for fraud or extortion, these sections stand on the sidelines and emphasize the absence of any broader legislative recognition of synthetic identity misuse.

Section 318 - Cheating

The "Bharatiya Nyaya Sanhita, 2023" (BNS), having superseded the previous Indian Penal Code, stands as a landmark enactment aimed at bringing forth comprehensive legislation that can propel the modernization of criminal law in India. The BNS keeps intact much of the structural and thematic basis of the IPC but amends them to directly tackle current-day crimes like those arising out of digital technologies. Though the Sanhita still retains some traditional provisions on cheating, fraud, and impersonation, it lacks express language to deal with issues arising from more nuanced threats coming from AI-based tools such as deepfakes. Impersonation of public officials using deepfake technology and manipulating victims into transferring money or providing personal information is a new type of cyber-enabled fraud that is giving a hard time in categorization in the existing legal paradigm. The BNS keeps the offences of cheating and personation at the core for prosecuting digital arrest scams, but the language of the statute has not yet evolved to take into consideration the layered complexity of synthetic media. As deepfakes increasingly become the tool of choice in impersonation frauds, it is imperative to ask if provisions such as "Section 318" and "Section 319" adequately cover AI-facilitated offenses. These provisions do, however, serve as the launching platform for legal intervention, but their operationalization demands a lot of interpretative exercises, judicial innovations, and investigatory acumen-areas where India is still yet to gain a firm footing in responding to AI orientated criminality.[13]

Section 319 - Cheating by Personation

Section 318 of the Bharatiya Nyaya Sanhita describes cheating as an act by which a person, being fraudulent and dishonest, deceives another, and thereby causes them to either transfer any property to any person or to do any act or omit any act which causes or is liable to cause injury. Specifically, "Section 318(4)" is about more serious cheating in which the fraud results in delivery of property or destruction or modification of any valuable security. Offending these crimes could be with punishment for a term which could extend to seven years or by fine or by both. This provision comes into play when instituted for AI-sourced digital arrest scams, whereby innocent victims are tricked into sending money to imposter government or law enforcement agents. Misled by deepfake video calls or audio synthesis calls, victims truly believe the urgency of the threat of prosecution or arrest and behave accordingly. They send money in the form of a fine or hand over precious information that culminates in loss of money. All of the essential elements of the section—deception, inducement, and transfer of property—are involved in these scams. Deception through a deepfake impersonation, however, makes it difficult to gather evidence. Detection and tracking of the mode of inducement are the primary evidence in building fraud; however, in digital arrest scams, the deployment of artificial media usually conceals the identity and geographical location of the scammer and hence makes it difficult to investigate. Therefore, probing these offenses requires stronger digital forensics with interpretive appreciation that AI-impostor impersonations are the species of the fraud or dishonest inducement contemplated by the phrase. Although the section is conceptually adequate, perhaps some procedural value and clear legislative direction need to be added to it to render it effectively appliable against AI-enhanced scams.

---

[12] Trishana Ramluckan, "Deepfakes: The Legal Implications", 19 *ICCWS* 282 (2024).

[13] Corporate AI Deepfake Fraud: Rising Threats and Regulatory Responses, *available at:* https://nquiringminds.com/ai-legal-news/Corporate-AI-Deepfake-Fraud-Rising-Threats-and-Regulatory-Responses/ (Visited on April 14, 2025).

Other Relevant Laws

Beyond the core provisions of the "Information Technology Act, 2000" and the "Bharatiya Nyaya Sanhita, 2023", other acts also add some insight to the regulatory framework relating to tackling deepfake impersonation in the context of AI-based digital arrest scams. These acts would not have been drafted with an emphasis on AI-generated identity fraud, yet they may hold some auxiliary legal grounds, depending on the circumstances of individual cases. Their relevance can change with respect to the type of content used, the impersonation, the source of the data, or the medium of transmission. These laws are indicative of the fragmented character of India's modern legal response to AI-based digital fraud. None of these have the ability to encapsulate the multi-layered techno-psychological manipulation involved in AI-based scams in isolation; however, together they are outlining the different avenues through which legal responsibility may be imposed and thus emphasizing the necessity of legislative convergence and consistency in this regard.

Apart from the general provisions of the "Information Technology Act, 2000", and "Bharatiya Nyaya Sanhita, 2023", certain other legal documents throw additional light on the regulatory aspect of rectifying deepfake impersonation in the arena of AI-based digital arrest frauds. These acts were never established to counter AI-based identity theft but may be applied on a collateral basis subject to each case. Depending on the range of content employed, impersonation used, source of information, and vehicle of communication, the pertinence of these acts is sure to differ. These acts continue to illustrate just how fragmented is the current Indian legal space when it comes to AI-facilitated digital deception. Calculated individually, none of these tools adequately addresses the technological plus psychological manipulations-in-layers constituting an AI-facilitated scam. Yet, they indicate the various forms through which liability can be proven and identify the need for a legislative convergence and clarity in this respect.[14]

The intent behind enacting the "Digital Personal Data Protection Act, 2023" was to protect personal digital data and thereby uphold the right to privacy within the ambit of Indian law on data. The Act delineates critical subjects such as "data principal" and "data fiduciary" to classify subjects and controllers of personal data. However, it contains an important exemption that substantially undermines the possibility of using this law to stop or punish deepfake impersonation. The exemption states that the Act does not intend to protect any information that is publicly disclosed by the data principal or is otherwise legally available in the public domain. From here on, one can guess the trouble. This exemption allows scammers that use publicly available pictures, videos, or social media content to feed their AI systems to circumvent the law. Since most data required to generate a deepfake is already available online, especially in the form of public speeches and social media profiles and news videos, the cover under this Act is thin. Using a person's image or likeness without their consent can be grossly immoral or traumatizing; however, this is only seen as a violation under the 2023 Act if such use is expressly unlawful under another statute. Therefore, individuals who are impersonated via publicly sourced content have limited legal protection under India's primary data-protecting law.[15]

While the Indian Penal Code, 1860, was repealed as a result of the enactment of the Bharatiya Nyaya Sanhita, 2023, incidences or offences occurring prior to the commencement of the new statute continue to be governed by the Code. In such instances, Section 416 of the IPC would be applicable dealing with cheating by personation, along with Section 420, which pertains to cheating and dishonestly inducing delivery of property. These provisions were directly old precedents of Sections 319 and 318 of the BNS, respectively, and bear more or less similar language and punishment. In the digital arrest scam-type of legacy cases where the deception happened before the new code came into force, the legal yardstick would be provided by these IPC sections. Their existence underscores the feeling that India is a transitioning legal system where more than one code may be in operation depending upon when the offence was committed. However, similar to their contemporary counterparts in the BNS, these IPC provisions are silent when it comes to specifying the mode of deception, either by traditional means or by AI. Courts may interpret such impersonation fairly broadly to include the realm of synthetic media; however, these provisions have limited effectiveness without an explicit statutory reference to AI-generated impersonation, especially in cases that require speedy disposition and thorough forensic analysis.[16]

Case Studies and Judicial Responses

The discussion around deepfake misuse also discusses legal protection under the Copyright Act, with limited applicability depending on the media used. Section 51 of the Copyright Act specifies that infringement is any unauthorized use of copyrighted material. Hence, in cases where a deepfake video contains copyright-protected content like an audio clip or visual design elements: say, a public address by a government official, a news broadcast, or a privately held video, the copyright holder may commence infringement proceedings. Such an application will be incidental, however, not directed toward the act of impersonation. The impersonator may use the content transformative in a manner that falls below the threshold of substantial reproduction, or they may claim fair use, parody, or a non-commercial usage intent, depending on context. Also, most of these impersonated public officials or persons will not have copyright ownership of widely circulated material that is used to synthesize their image or voice. This makes enforcement under the Copyright Act further difficult, except perhaps where corporations or media houses whose proprietary content is misappropriated for scam-based purposes. Even where it can be applied, remedies under the Act are essentially civil-oriented-injunctions, damages, and accounts of profit-rather than criminal penalties, which can curb such activity by scammers working across jurisdictions and by means of digital anonymity. Hence, while the Copyright Act theoretically carves out some space to contest certain uses for deepfakes, it falls short, in scope and intent, as a remedy against identity deception.[17]

[14] Fabian Muhly, Emanuele Chizzonic, et.al., "AI-deepfake scams and the importance of a holistic communication security strategy", 6 *ICLR* 53 (2025).

[15] Amrutha Bharathan Karamvalappil, "The Revolution of Digital Scams and Right to Privacy in India", 7 *IJFMR* 1 (2025).

[16] Rajesh J Ovhal, "Deepfakes – Serious Threat in Context of India", *available at:* https://www.globalscientificjournal.com/researchpaper/Deepfakes_Serious_threat_in_context_of_India.pdf (Visited on April 14, 2025).

[17] Balasubramani Murugesan, "AI-Driven Phishing And Deep Fakes: The Future Of Digital Fraud", *Forbes*, March 10, 2025.

Notable Cases Involving Deepfake Scams

Judicial engagement with AI-generated deepfakes in India is still in its formative stage. However, in recent years, there has been a slow rise of judgments and legal proceedings going to show the growing consciousness of the technological threat. Courts have begun responding to the misuse of AI in the context of impersonation and personality rights, particularly where celebrity images are misappropriated. Thus, though there is not yet any penal legislation that specifically deals with deepfakes, the courts have been inclined to apply existing doctrines of law under the Information Technology Act, 2000 and the right to privacy as embodied by Article 21 of the Constitution. By-and-large, the judicial treatment of deepfake technology remains limited to civil relief such as injunctions, and very little has come about in criminal jurisprudence in cases of scams. Digital arrest scams, while ruinous in terms of social impact, have so far not been the subject of any settled judicial pronouncements, especially because of procedural difficulties-in-gathering evidence, identifying offenders, and jurisdiction. This segment reviews some significant precedents and ongoing probes to understand the attempts of courts and police authorities in negotiating these novel challenges.[18]

If we rank deepfake misuse cases chronologically, the Anil Kapoor 2023 litigation has to come first on the list as one of the prime cases in the deepfake jurisprudence, featuring the DHC issuing an injunction against unauthorized usage of the actor's name/image/voice through technological means, including deepfakes. The case thus was a landmark in recognizing personality rights and putting a spotlight on the growing concern of AI-generated media. Not concerning a financial scam or an impersonation set to defraud the public, nonetheless, the court's recognition of deepfake technology and how it can be harmful to reputation and privacy stands critical, as it set a precedent where it was surmised that unlike in case of statutes dealing with privacy or misappropriation per se, the personality of an individual is protected under a far broader umbrella and thus protected in its own right; deepfakes or no deepfakes. Along similar lines, in 2022, the Delhi High Court granted interim relief on a petition Likewise filed by Amitabh Bachchan for the unauthorized usage of his name, voice, and image. The Court proclaimed that the actor is entitled to prevent unauthorized commercial exploitation of his persona, thus carving judicial space for future instances of manipulated digital content, although this judgment too was aimed toward personality rights and reputation as opposed to criminal wrongs.[19]

Judicial Interpretations and Challenges

Among digital arrest scams, the one that has been observed in Mumbai between 2024 and 2025 has been truly showstopping in nature. An 86-year-old woman was cheated out of ₹20.25 crore in a very sophisticated operation where the scammers had misrepresented themselves as the police using digital technology, including some video calls that appeared to be deepfakes. The case was likely being framed against her for money laundering, so she was persuaded to remit money in multiple transactions over a period of weeks. The verdict on this case is yet to come, but the police probe demonstrates the extent of technological manipulation at play and the grave psychological trauma attributed to the victim. This case is a dark warning of the power of deepfake-based fraud and of the prosecutorial ineptness on the other side, when even law enforcement agencies cannot verify the digital evidence and track down the culprits. In yet another Kerala case in 2023, a senior citizen was swindled of ₹40,000 following a video call received from an imposter who claimed to be the victim's previous colleague. Deepfake technology, purportedly deployed to mimic the face and voice of the caller, is still under investigation, highlighting the enforcement difficulties presented by such cybercrime. The police confirmed they needed forensic specialists to verify whether the video was actually a deepfake, so even in this relatively modest scam, procedural barriers were placed before speedy judicial recourse. These incidents attest to the technical sophistication of such cybercrooks, but also point to the urgent need for modernization of the investigative process, judicial specialization, and legislative foresight.

Judicial interpretation of deepfake-related offences in the Indian setting has largely been shaped through privacy rights and unauthorized use of images. Courts have tended to grant interim relief in personality rights cases using tort law principles, Section 66E of the Information Technology Act, 2000 (violation of privacy), and Article 21 of the Constitution as guiding bases. But the absence of judicial pronouncement is glaring in cases involving digital arrest scams, where the impersonation is supposedly facilitated through AI-generated media. The lacuna exists partly due to these offences being rather novel and partly due to the complicated evidentiary standard that discourages quick judicial intervention. While the court has exhibited some inclination towards engaging with the subject matter, the interpretation has so far remained restricted to civil domains, primarily reputation-related remedies and less so on criminal or deterrent measures. Courts are under no legal obligation according to current law to draw a distinction between impersonation carried out by a human or one using synthetic content generated by an AI tool. Therefore, even if the judiciary accepts that deepfakes cause harm, it remains statutorily freer to deal with such offences, via the penal mechanism, only if the acts fall squarely within well-established penal categories.[20]

Conclusion

The development of AI-designed digital arrest scams has shed light on some glaring gaps in India's law and enforcement apparatus. Deepfakes power these scams, and they represent a nasty cocktail of psychological coercion and technological trickery with extremely sophisticated challenges that the previous laws cannot deal with. Impersonating public servants and law enforcement officers via synthetic media begets a new form of identity theft, which is interactive, dynamic, and nearly indistinguishable from reality. By being asked to lose money, victims are in fact being duped through coercion

[18] A. Broinowski, F. R. Martin, et.al., "Beyond the deepfake problem: Benefits, risks and regulation of generative AI screen technologies", 0 *MIA* 0 (2024).

[19] Jon Bateman, "Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios", *available at:* https://carnegieendowment.org/research/2020/07/deepfakes-and-synthetic-media-in-the-financial-system-assessing-threat-scenarios?lang=en (Visited on April 18, 2025).

[20] Kinza Yasar, Nick Barney, et.al., "What is Deepfake Technology?", *available at:* https://www.techtarget.com/whatis/definition/deepfake (Visited on March 12, 2025).

by synthetic state power, which injures not only personal dignity but collective trust in digital governance as well. Overlapping the spaces of AI and criminal personation is an endeavor requiring more than simply the deployment of conventional provisions against cheating and personation; it requires creating a legal acknowledgment of synthetic identity as a new category of harm that cannot be adequately redressed by liberal readings of outdated penal terminology. Whereas Sections 66D of the Information Technology Act, 2000, and Sections 318 and 319 of the Bharatiya Nyaya Sanhita, 2023, offer a solution, their current nomenclature and scope do not reflect the essence and the challenges of AI-facilitated deception accurately.

As AI brings in a new age of digital arrest scams, cracks in the legal and enforcement mechanism of India are beginning to show. As a deepfake-driven scam, the scams combine psychological manipulation with tech-based deceit to present issues that regular laws are not capable of untangling. With synthetic media, impersonation of the police and public agents turns into a distinctive form of theft that is dynamic, interactive, and on the verge of being indistinguishable from life. While governments steal money from victims, they impersonate state power to lower human dignity and contaminate the public trust in online governance. The AI identity theft raises an issue beyond simply the use of deception and impersonation. It requires a clear legal acknowledgment of synthetic identity as a distinct form of harm that cannot be handled by loose readings of penal terminology long outdated. While the existing laws, i.e., Section 66D of the Information Technology Act, 2000 and Sections 318 and 319 of the Bharatiya Nyaya Sanhita, 2023, point the direction forward, they are all too poorly matched and short in order to encapsulate the subtle technicalities that come with AI-mediated deception.

Procedural and evidentiary issues only add to inherent limitations in the legal system. Demonstrating someone to be using a deepfake would involve digital forensics; however, such technical know-how is rare among Indian police forces and forensic laboratories. Synthetic media, under the "Bharatiya Sakshya Adhiniyam, 2023", has to be tested in court. However, it becomes problematic without clear-cut procedures regarding the verification of AI-generated material. The newness of the invention, and the way it evolves speedily, makes judges and the police disadvantageous. The judiciary stands a serious chance of conflicting verdicts in the face of a lack of sufficient training and consultation with experts, which would only weaken the power of the law to deter. Additionally, jurisdictional boundaries are a larger obstacle as frauds mostly function outside Indian territorial jurisdiction. While the IT Act and the BNS grant extraterritorial jurisdiction, the usability of this jurisdiction hinges entirely on diplomatic cooperation, mutual legal assistance treaties, and transnational enforcement mechanisms-still in their nascent stage. This reliance for aiding investigation and extradition itself gives rise to procedural delays, leaving the perpetrators free from punishment in time.

Lastly, the legal system needs to balance safeguarding rights of individuals and promoting technological innovation. Not every application of deepfake technology is harm, and excessive regulation can curtail valid artistic, educational, or journalistic applications. Legislation needs to be narrowly directed towards clear definitions of bad intent and proportionate punishment of such intents. In this way, AI-powered digital arrest scams are not merely in the anomaly of the law but point towards a deeper transformation in the role of identity, authority, and trust in the digital era. Indian law must adapt along with that of the challenge, not in isolated doctrinal change but in a coordinated and visionary rebuilding of the interface between criminal law and artificial intelligence. Otherwise, its process is to continue being reactive and not systematic, unable to protect citizens from the new dangers of AI-enabled deception.