DEEPFAKES AND IDENTITY APPROPRIATION: RE-EXAMINING THE LIMITS OF INDIAN CRIMINAL LAW IN THE AGE OF GENERATIVE AI

Kunduru Venkata Nandini, School of Law, Woxsen University

ABSTRACT

Rapid advances in generative artificial intelligence have enabled the creation of highly realistic synthetic videos, audio, and images capable of imitating a person's face, voice, and likeness without consent.[1] Public discussions on deepfakes are usually about misinformation, but this paper argues the fundamental legal problem lies elsewhere: Indian criminal law which treats deepfakes as wrongful only when they produce a separate recognisable harm such as fraud, defamation, or fabricated evidence rather than recognising it as the theft of identity of an individual as an independently wrongful act. Drawing on recent Indian incidents which include Rashmika Mandanna deepfake controversy, deepfake-enabled investment scams impersonating executives associated with Bombay Stock Exchange (BSE), and AI-generated political content circulated during the Tamil Nadu Assembly Election 2026, this paper examines the Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023, and Digital Personal Data Protection Act, 2023, and finds that each statute applies only after a downstream consequence occurs. The paper then discusses Indian personality rights law, which recognises that using someone's identity without consent is independently illegal and can be enforced through civil courts. It argues that this principle should also be applied in criminal law, not just civil law. The paper further recommends creating a new law that specifically criminalises the non-consensual use of digitally created or synthetic versions of a person's identity such as deepfakes. Overall, the paper suggests that Indian law should shift from a reactive approach in which action is taken only after harm occurs to a preventive approach where unauthorized use of identity itself is treated as an offence. This paper's novel contribution lies in reframing deepfake regulation in India from a consequence-based harm model to an identity-based appropriation model, arguing that unauthorised digital replication itself should be treated as the primary criminal wrong.

Keywords: Deepfakes, Artificial Intelligence, Identity Appropriation, Criminal Liability, Personality Rights, Data Protection Law, Digital Privacy

[1] IBM AI Deepfake Overview

Introduction

Deepfakes are a form of synthetic media capable of generating face-swapped videos, lipsynced audio overlays, voice cloning, full-body reenactment, and text-based conversational clones.[2] Deepfake systems primarily rely on Generative Adversarial Networks (GANs)[3] and use advanced machine learning models trained on large datasets of audio, image and video inputs. Unlike traditional forms of impersonation, deepfakes use AI to create highly realistic representations that are often indistinguishable from authentic human expression, making it much harder to detect.

Deepfake technology has become easy to access because many tools are now freely or cheaply available, such as apps that swap faces, open-source AI models, voice-cloning software, cloud computing tools, and simple consumer apps. These tools have lowered the technical skill needed to create deepfakes. Earlier, only experts could make such content, but now even ordinary users can create and share realistic fake videos or audio quickly and easily.

The misuse of deepfakes results in fraud, impersonation, defamation, financial scams, and fabricated evidence. More importantly, synthetic media such as deepfakes is not just about spreading false information. It involves copying a real person's identity features—such as their face, voice, and appearance—without permission. This creates legal issues that are more serious than normal misinformation. However, most existing laws were enacted before the emergence of AI technology, so they may not adequately address problems caused by AIbased identity replication.

Indian criminal law mainly focuses on punishing the consequences of deepfakes, such as fraud, defamation, or fake evidence. However, it does not directly criminalise the initial act of using someone's face, voice, or identity without consent, which is what enables those harms in the first place. Because of this, the law does not clearly deal with the act of identity misuse itself.

The paper proceeds as follows. Part II examines the technological nature of deepfakes and the threat landscape they have created, illustrated through three recent Indian incidents. Part III maps the existing legal framework under the Information Technology Act, 2000,[4] the

[2] Britannica Artificial Intelligence Overview
[3] NVIDIA GAN Explanation
[4] Information Technology Act, 2000

Bharatiya Nyaya Sanhita, 2023,[5] and the Digital Personal Data Protection Act, 2023.[6] Part IV develops this paper's central argument: that Indian law's consequence-triggered structure leaves unauthorised appropriation of identity unaddressed at the moment it occurs. Part V

turns to Indian personality rights jurisprudence as a doctrinal model that already treats appropriation as independently wrongful. Part VI offers concrete legislative recommendations, and Part VII concludes.

Technology and the Threat Landscape

Before examining the adequacy of Indian law, it is necessary to understand the technological nature of deepfakes and the expanding threats that existing legal frameworks increasingly struggle to address.

Deepfakes can be divided into four broad categories: face-swapped videos, voice cloning, full-body reenactment, and text-based conversational clones. While early deepfake systems primarily relied on Generative Adversarial Networks, modern synthetic media generation increasingly uses advanced machine learning models trained on large datasets of audio, image, and video inputs. Unlike traditional forms of impersonation, deepfakes use artificial intelligence to generate hyper-realistic synthetic representations that are often indistinguishable from authentic human expression, making it much harder to detect. What has changed in recent years is not only the technique itself but also its accessibility. Tools that once required research-level expertise are now widely accessible, significantly lowering the technical barriers to creating highly realistic synthetic media.

Three recent incidents in India illustrate how this easy accessibility to deepfakes is leading to real harm, and how the type of harm depends on the person targeted and the intention behind it.

The first is the deepfake video of actor Rashmika Mandanna, which went viral in November 2023, manipulating an unrelated video to substitute her face onto another woman's body. Mandanna herself, in a public statement, described the incident in a way that strongly supports the central argument of this paper she called it "identity theft." Yet the legal response that

[5] Bharatiya Nyaya Sanhita, 2023
[6] Digital Personal Data Protection Act, 2023

followed was built around forgery and reputational harm, not around the unauthorised replication of her likeness as a wrong in its own right.[7]

The second incident shows the same pattern in a financial setting. Beginning in early 2026, the Bombay Stock Exchange issued repeated public warnings at least four by April 2026 about a deepfake video of its Managing Director and CEO, Sundararaman Ramamurthy, falsely shown offering stock tips and guaranteed returns. The video directed viewers to WhatsApp channels promising extraordinary profits, a pattern that mirrors a broader wave of deepfake-enabled investment fraud documented by Mumbai Cyber Police,[8] which recorded hundreds of complaints and losses running into hundreds of crores of rupees in 2025 alone. Even in such situations, legal responses are triggered only after harm occurs. The Bombay Stock Exchange (BSE) can warn people or ask platforms to remove the fake content, but the law does not directly punish the act of using Ramamurthy's face and voice without permission to create a fake endorsement. Instead, legal action is triggered only when that fake content leads to actual fraud, such as people being tricked into investing money.

The third incident is more diffuse but arguably more consequential for democratic processes.

During the 2026 Tamil Nadu Assembly election, an AI-generated video resurrected former Chief Minister C.N. Annadurai, who died in 1969, complete with his voice and speech patterns, to endorse a party that did not exist during his lifetime. The video spread for hours before it was identified as synthetic, by which point it had already reached a wide audience. A broader fact-checking review of the same election cycle found at least nineteen AI-generated videos circulated across Tamil Nadu and three other states without the disclosure required under the amended IT Intermediary Rules notified that February.[9] The Election Commission of India acted on thousands of flagged posts during the cycle, but its intervention like BSE's warnings and the Delhi Police's response in the Mandanna case came only after the synthetic content had already circulated and caused its effect.[10]

These three cases, drawn from different domains such as entertainment, finance, and elections, all show the same pattern. In each case the law only stepped in after the deepfake caused clear harm such as damage to reputation, financial loss through fraud, or spreading false political

[7] Rashmika Mandanna Deepfake Video Goes Viral, *The Indian Express* (November 2023).
[8] Deepfake investment scams rise in India,*The Economic Times* (2025–2026 reports on cyber fraud trends).
[9] AI-generated videos circulate during Tamil Nadu election cycle, *The Hindu* (2026).
[10] Election Commission of India

information. However, simply using a person's face or voice without permission to create the deepfake was not enough on its own to trigger legal action. This gap is what the next section will discuss.

The Existing Indian Legal Framework

Before examining whether Indian law adequately addresses deepfakes, it is necessary to examine the current legal provisions which are available to victims and to ask at each stage what triggers their application.

Firstly Section 66C of Information Technology Act, 2000 punishes identity theft the fraudulent or dishonest use of another person's password, electronic signature, or other unique identifying feature while Section 66D punishes cheating by personation through a computer resource. Both provisions, however, require either a fraudulent intent or an act of cheating; neither contemplates the creation of a synthetic likeness as a wrong independent of what is done with it. Section 66E, which punishes the unauthorised capturing, publishing, or transmission of images that violate a person's privacy, comes closer to addressing appropriation directly, but its scope is largely limited to images of private or intimate areas, leaving ordinary face-swap or voice-clone content but it does not fully cover common deepfakes that misuse someone's face or voice without consent[11]. This is the main gap that surfaced in the Rashmika Mandanna case where the Delhi police invoked sections 66C and 66E of the IT Act along with the section 465 and 469 of the Indian Penal Code[12] (forgery, and forgery to harm reputation), but the charges were framed around forgery and reputational harm, not around the unauthorised digital replication of her likeness as such.

The Bharatiya Nyaya Sanhita, 2023 (which replaced the Indian Penal Code) keeps the same basic approach to these issues instead of changing it in a major way. The offence of forgery, previously spread across Sections 463 to 471 of the IPC, has been consolidated under Section 336 of the BNS, while cheating previously Sections 415 to 420 of the IPC is now consolidated under Section 318, with graded punishment depending on the degree of harm caused to the victim. Defamation, previously Sections 499 and 500 of the IPC, is now Section 356 of the BNS.[13] Each of these provisions remains organised around a downstream harm: forgery

[11] Information Technology Act 2000, ss 66C, 66D, 66E.
[12] Indian Penal Code Sections 465, 469
[13] Bharatiya Nyaya Sanhita 2023, ss 318, 336, 356.

requires an intention to cause damage or injury, cheating requires inducement and resulting harm, and defamation requires injury to reputation but none of them treats the unauthorised digital replication of a person's face or voice by itself as the relevant wrong. A deepfake created but never circulated would fall outside all three provisions even though appropriation of the victim's identity has already occurred at the moment of creation.

The Digital Personal Data Protection Act, 2023 (DPDP Act)[14] at first seems like it could solve the deepfake problem because it controls how personal data is collected and used. This includes personal digital information like images or voice data which can be used to train AI models. In theory, using someone's face or voice to train a deepfake system without their permission would violate the requirement of consent under Section 4 of the Act.

However, in reality, this law is not designed to punish individuals who create or spread deepfakes. It is a civil and regulatory law, meaning it mainly imposes fines on organizations or data handlers through a regulatory authority (Data Protection Board), not criminal punishment for individuals making deepfakes.

Also, the law assumes that data is processed by identifiable organizations or companies, not by anonymous individuals using personal devices. Because of this the law does not effectively deal with real-world deepfake creation and misuse.

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code)

Amendment Rules, 2026[15] (notified on 10 February 2026 and effective from 20 February 2026) are the first major legal step in India that directly recognizes that AI-generated or synthetic content needs special regulation. These rules introduce a new category called "synthetically generated information." They require platforms that create or host such content to clearly label it and attach secure metadata so it can be traced. They also require that illegal synthetic content be removed very quickly—within three hours. However, these rules mainly place duties on online platforms and intermediaries, not on individuals who actually create deepfakes. The focus is on labelling and removing content after it appears online not on punishing the person who made the deepfake. Because of this there is still a gap as seen during the Tamil Nadu elections deepfakes can spread and influence people before platforms detect them and take

[14] Digital Personal Data Protection Act 2023, s4
[15] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules 2026.

them down.

The Consequence-Triggered Problem

The previous section showed that India's three main laws on this issue share one common pattern. This section now clearly identifies that pattern and explains why it creates an important gap or weakness in the legal system.

For this paper, "unauthorised appropriation" means using AI to take or copy someone's identity without permission such as their face, voice, appearance, or digital identity and recreating it digitally no matter what is later done with it. This is different from crimes that Indian law already recognizes, like fraud, cheating, defamation, or creating fake evidence. Those laws deal with how the deepfake is used and what harm it causes. In other words, unauthorised appropriation of identity and the subsequent harmful use of that identity are legally distinct issues.

For example, if someone creates a deepfake video using another person's face and voice but if they don't use it for fraud, money, or public sharing. In such a situation, the person may not attract liability under the Bharatiya Nyaya Sanhita or the Information Technology Act. DPDP Act may apply only through regulatory action, not criminal punishment.

Deepfakes are fundamentally different from ordinary forms of impersonation, and this difference is legally important. In traditional impersonation, such as forging a signature or pretending to be another person, the harmful act usually occurs at the moment the deception is carried out. Deepfakes, however, operate differently. Once a synthetic replica of a person's face or voice is created, it can be permanently stored, copied endlessly, transferred anonymously across digital platforms, and reused by multiple individuals beyond the control of the original creator. This means the interference with a person's identity begins at the stage of creation itself, even before the deepfake is publicly shared or used to cause any further harm.

Some people might argue that "This is normal in criminal law because laws usually punish harm, not intention or creation." However, deepfake technology differs fundamentally from conventional forms of impersonation. Once created, a deepfake can be reused by anyone, anytime. So the harm starts at the moment of creation, not just when it is used.

The real issue is not just harm caused by deepfakes. The deeper legal problem is that Indian

law does not treat unauthorised digital replication of identity as an independent criminal wrong. Existing legal provisions mainly address the consequences of deepfake misuse, such as fraud, defamation, or deception, but they fail to recognise that unauthorised digital appropriation itself constitutes an independent invasion of personal autonomy and identity deserving direct legal protection. This raises the question of whether any existing doctrine in Indian law already treats identity appropriation in this manner and whether it offers a possible model for the criminal law reform this paper argues is necessary. That question is taken up in the next section.

Toward an Appropriation-Triggered Model: Lessons from Personality Rights

The previous section highlighted an important weakness in Indian criminal law: legal action is generally triggered only after a deepfake causes harm, rather than at the stage where a

person's identity is copied without permission to create the deepfake. This section examines whether Indian law already contains any doctrine that treats such unauthorised use of identity as wrongful in itself. It finds that such recognition does exist, although currently outside criminal law.

In India, personality rights have mainly developed through civil litigation. Initially, these rights emerged through passing off claims and were later expanded through judicial recognition of privacy and proprietary interests connected to an individual's identity. In ICC Development (International) Ltd. v. Arvee Enterprises,[16] the Delhi High Court held that the right of publicity belongs only to an individual and cannot be claimed by a corporate entity. Even though the plaintiff did not succeed, the judgment was significant because the Court recognised that rights over one's name, likeness, voice, and other identity attributes flow from privacy itself. The important point here is that the legal wrong begins with the unauthorised use of identity, not merely with any later financial or reputational harm.

This principle was strengthened in Titan Industries Ltd. v. Ramkumar Jewellers.[17] In this case, the Delhi High Court granted an injunction against the unauthorised commercial use of Amitabh Bachchan and Jaya Bachchan's images. The Court held that individuals have the right to decide how and when their identity is used commercially. What mattered most was that the

[16] *ICC Development (International) Ltd v Arvee Enterprises and Anr*, 2003 SCC OnLine Del 2 (Delhi High Court, 1 January 2003).
[17] *Titan Industries Ltd v M/s Ramkumar Jewellers*, 2012 SCC OnLine Del 2946 (Delhi High Court, 26 April 2012).

persons were clearly identifiable, not whether the use had caused consumer confusion or some separate harm. This shows a very different legal approach, where the wrongful act is the unauthorised use of identity itself.

The relevance of this principle to deepfakes became even clearer in Anil Kapoor v. Simply Life India & Ors..[18] In this case, the Delhi High Court dealt directly with defendants who had used generative AI to create deepfake content involving Anil Kapoor, including manipulated videos, synthetic voice clips, and other AI-generated content using his likeness. The Court issued an injunction stopping the unauthorised use of his name, image, voice, and persona through AI tools. Importantly, the Court granted relief without requiring proof of fraud, deception, or reputational damage. This showed that simply replicating someone's identity without permission was treated as legally significant.

Taken together, these decisions reveal an important principle within Indian law: an individual's identity has independent legal value, and interference with that identity can itself justify legal protection.

This idea is also supported by constitutional law. Although personality rights developed mainly through private law remedies, their foundation increasingly rests on the idea that identity deserves legal protection in itself. In Justice K.S. Puttaswamy v. Union of India,[19] a nine-judge bench of the Supreme Court of India held that privacy is a fundamental right protected under Article 21 of the Constitution as part of the right to life and personal liberty. Courts have repeatedly connected personality rights to this constitutional principle, recognising that a person's name, voice, and likeness deserve protection because unauthorised control over them violates the same dignity interests protected by privacy rights. This matters because it shows that Indian law already has the conceptual basis to treat identity appropriation itself as the legal wrong, even though this recognition currently exists outside criminal law.

However, this doctrine cannot by itself solve the deepfake problem. Personality rights cases mainly provide civil remedies such as injunctions, damages, or takedown orders, which usually require significant resources and access to urgent civil litigation, as seen in the cases discussed above. These remedies do not create criminal punishment, impose custodial liability, or provide an easily accessible remedy for ordinary individuals targeted by deepfakes. What these

[18] *Anil Kapoor v Simply Life India & Ors*, CS (COMM) 652/2023 (Delhi High Court, 20 September 2023).
[19] *Justice KS Puttaswamy (Retd) v Union of India*, (2017) 10 SCC 1.

cases clearly establish, however, is the core principle that nonconsensual replication of a person's identity is independently wrongful, even when no fraud, defamation, or confusion has yet occurred. The real reform needed, therefore, is to bring this principle into criminal law rather than leaving it limited to civil remedies that are mostly available only to well-resourced individuals.

Recommendations

The discussion in the previous sections shows that what is required is not simply stricter enforcement of existing laws, but a targeted legislative response that directly addresses the legal gap identified in this paper.

The most important reform would be the introduction of a separate statutory offence that specifically criminalises the non-consensual or unauthorised creation of synthetic replicas of another person's face, voice, likeness, or biometric identity through artificial intelligence systems. Such a provision would give effect to the appropriation-based approach discussed in Part V by making legal liability arise at the moment an individual's identity is digitally replicated without permission. This would reflect the principle already recognised by Indian courts in personality rights cases, but instead of limiting protection to civil remedies, it would bring the issue directly within criminal law. At the same time, the law must be drafted carefully so that legitimate uses such as satire, parody, authorised AI research, or consensual use of identity are clearly excluded. The main objective should remain preventing the unauthorised digital use of another person's identity.

A second reform would be to amend Sections 66C and 66D of the Information Technology Act so that they expressly include AI-generated impersonation and synthetic identity misuse. At present, both provisions largely depend on fraudulent or dishonest intent, language that was framed long before generative AI made it possible to imitate another person without necessarily carrying out an immediate fraud. A direct legislative amendment would therefore be more effective than leaving courts to interpret provisions that were enacted in a completely different technological environment.

The repeated pattern seen in the BSE deepfake incident and during the Tamil Nadu election cycle also highlights the need for a faster emergency takedown mechanism. Such a system should allow victims, authorised government agencies, or recognised reporting bodies to file

verified complaints that can trigger immediate action, without forcing victims to first prove fraud, defamation, or some other legally recognised harm. Since there is always a possibility that complaint systems may be abused to silence legitimate content, safeguards must also exist. A better approach would be temporary immediate removal followed by a short verification process, with restoration if the complaint turns out to be unsubstantiated.

A fourth reform concerns stronger technological regulation. The provenance watermarking obligations introduced under the 2026 IT Amendment Rules should be expanded further.[20] AI-generated content should carry traceable and tamper-resistant metadata from the moment of its creation. This would directly address the current weakness in the law, where legal obligations mainly begin once the content has already entered circulation. Although enforcing such requirements against fully decentralised open-source systems may be difficult, the obligation should at least apply to commercial AI companies and publicly accessible generative AI platforms operating within India.

Fifth, platform liability rules should also be strengthened. Platforms that knowingly continue hosting harmful deepfake content even after receiving verified notice should face clear statutory penalties instead of relying only on the relatively weak due diligence obligations under the present intermediary framework. This may require reconsidering the safe harbour protections currently available under Section 79 of the Information Technology Act, because allowing platforms to remain immune even after failing to act would undermine any stronger liability framework. Stronger liability rules would also make the existing three-hour takedown standard more effective by giving it actual legal consequences instead of leaving it as a procedural requirement. Section 79 immunity should be made conditional upon immediate compliance with verified deepfake removal notices.

Taken together, these reforms would shift Indian law away from its present reactive approach, where legal action begins only after harm occurs, and toward a preventive framework that recognises unauthorised digital replication of identity as the primary legal wrong. In the context of deepfake technology, the unlawful capture and synthetic recreation of a person's identity should itself be treated as the central harm, rather than only the later consequences that may follow from it.

[20] Ministry of Electronics and Information Technology

Conclusion

This paper began with a central argument that Indian criminal law addresses deepfakes only when they lead to some separate and identifiable harm, but does not recognise the unauthorised use of a person's face, voice, or likeness for creating a deepfake as an independent legal wrong. The three incidents discussed in Part II the Rashmika Mandanna deepfake controversy, the BSE CEO investment scam, and the Tamil Nadu election deepfakes demonstrated how this pattern exists across different sectors, including entertainment, finance, and democratic processes. The legal analysis in Part III further showed that the same pattern exists under the Information Technology Act, the Bharatiya Nyaya Sanhita, and the Digital Personal Data Protection Act, all of which respond only after fraud, defamation, forgery, or some regulatory violation has already occurred rather than at the stage where the deepfake is actually created.

Part IV argued that although criminal law generally works on a consequence-based model, this approach is not fully suitable in the context of deepfake technology. Unlike ordinary impersonation, a deepfake once created can continue to exist independently and may later be copied, stored, circulated, or misused long after its original creation. Part V demonstrated that Indian law already contains a possible legal foundation to address this issue. Through personality rights jurisprudence, particularly in the Anil Kapoor case, courts have already recognised that unauthorised replication of a person's identity can itself be legally significant even without proof of later fraud, deception, or reputational damage. What remains missing, however, is bringing this principle from civil law into criminal law where it can provide a more accessible remedy.

The five recommendations proposed in Part VI introducing a separate offence for nonconsensual synthetic replication, expanding provisions under the Information Technology Act, creating a verified emergency takedown mechanism, strengthening provenance watermarking requirements, and revisiting platform liability rules are intended as an initial framework rather than a complete solution. As generative artificial intelligence becomes increasingly accessible, the central concern raised in this paper will become even more urgent. Indian law must begin recognising that the unauthorised digital replication of a person's identity is itself the primary legal wrong, instead of waiting to intervene only after further harm has already occurred.

Bibliography

A. Statutes

1. Information Technology Act, 2000.
2. Bharatiya Nyaya Sanhita, 2023.
3. Digital Personal Data Protection Act, 2023.
4. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026.
5. Constitution of India.

B. Cases

1. Anil Kapoor v. Simply Life India & Others.
2. Titan Industries Ltd. v. Ramkumar Jewellers.
3. ICC Development (International) Ltd. v. Arvee Enterprises.
4. Justice K.S. Puttaswamy v. Union of India.

C. News Reports / Online Sources

1. The Indian Express Report relating to Rashmika Mandanna Deepfake Controversy (2023).
2. Business Standard Reports regarding Bombay Stock Exchange deepfake investment scam warnings (2026).
3. The Hindu Coverage relating to AI-generated political content during Tamil Nadu Assembly Election (2026).
4. Press Information Bureau, Government of India Notifications regarding IT Rules and synthetic media regulation.

5. Election Commission of India Reports and notices relating to AI-generated election misinformation.

D. Secondary Sources

1. Research articles on Artificial Intelligence and Deepfake Regulation.
2. Academic literature on Personality Rights and Privacy Law in India.
3. Legal scholarship on Criminal Liability for Digital Identity Misuse.
4. Journal articles relating to AI Governance and Synthetic Media Regulation.