



The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

STOLEN FACES: NAVIGATING THREATS TO ONE'S DIGITAL IDENTITY IN THE AGE OF AI

-Asmaa Barwelkar

We've all seen the ads: our favourite celebrities endorsing a brand, looking as authentic as ever. Later, we find out it wasn't really them at all—deepfakes and artificial intelligence are turning digital identity theft into an accessible reality. Unlike Photoshop and editing tools used to make fabricated images, Artificial intelligence (AI) uses technology like face morphing and voice cloning to replicate one's personal traits – looks, voice, likeness. This makes it harder for digital audiences and consumers to distinguish between real people and AI-generated ones.

AI uses Generative Adversarial Networks (GANs) to overlay one person's face onto another's body in videos and images or to deepfake one's voice into another in the creation of a hoax audio to deceive people. When AI is prompted to be used to replicate one's identity, it strips away the individual's autonomy and public identity across digital platforms. Infringing the 'Right to Privacy', although not explicitly mentioned in the Indian Constitution, the Right to Privacy is recognised as an intrinsic part of the Right to Life and Personal Liberty under Article 21, as decided in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017)¹.

The most prominent example can be seen in scams done with the help of AI avatars that are made to resemble real people, giving a false impression that an actual human favoured the product being sold. AI influencers, for example, online influencer Lil Miquela has over three million followers on Instagram alone, while Lu do Magalu has over fourteen million followers; they present themselves as fashion, lifestyle, art, and health gurus for the sole purpose of advertising and selling products, ultimately deceiving and misleading the consumer.²

¹ INDIA CONST. art. 21; *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1.

² Jeannie Marie Paterson, AI Mimicking and Interpreting Humans: Legal and Ethical Reflections, 22 J. BIOETHICAL INQUIRY 539, 542 (2025).

There are some legal remedies available under the Intellectual Property laws and the DPDP Act, but they fail to address the underlying issues relating to identity theft by AI. For example, Section 66(c) & 66(d) of the IT Act, 2000, related to identity theft and cheating by impersonation, are only applicable to cases of fraud and cheating. For instance, if a brand uses a deepfake to create a commercial Ad without the intent to commit fraud, and makes no false claims, merely using it to mimic a celebrity's likeness for commercial gain, it will fall outside its scope. While Indian copyright and trademark laws grant artists 'Performers Rights' and prohibit registration of trademarks on living persons' names and likenesses, they still fail to fully protect a person's personal traits from AI exploitation; the DPDP Act of 2023 requires explicit consent to process biometric data, though it still falls short of regulating the actual generation of synthetic deepfakes.³

E.g., in *Anil Kapoor v. Simply Life India & Ors.*, the Delhi High Court passed an ex parte injunction protecting the actor's personality rights against AI-generated deepfakes, unauthorised merchandise, and domain squatting. Immediately stopping the unauthorised usage of the name 'Kapoor' in domain names, misuse of his signature catchphrase 'Jhakhaas,' and broadly restrained 16 entities, and the world at large, from using his name, likeness, image, and AI-based content like Ads and GIFs for commercial gain. Also issued John Doe orders against anonymous and future infringers.⁴

Beyond celebrities' infringement of personality rights, greater risks from synthetic media are faced by the general public in situations like private photos morphed into fabricated sexual content for harassment, sextortion, or revenge, affecting women and, in some cases, minors. Scams like 'Digital Arrest' and family emergency scams, and unauthorised KYC checks, expose people to financial fraud and identity theft. While the IT Rules mandate labelling AI-generated content to curb misinformation, these disclosures are often ignored by malicious actors or bypassed by consumer psychology, where a synthetic image can make people ignore all the technical warnings.⁵ A person is bound to face some reputational or commercial harm, or both, due to the malicious intent of another in creating fake content using AI that fabricates one's reality on a digital platform.

³ Information Technology Act, No. 21 of 2000, § 66C; Information Technology Act, § 66D; Copyright Act, No. 14 of 1957, § 38; Trade Marks Act, No. 47 of 1999, § 14; The Digital Personal Data Protection Act, 2023, § 6, No. 22, Acts of Parliament, 2023 (India).

⁴ *Anil Kapoor v. Simply Life India & Ors.*, CS(COMM) 652/2023, I.A. 18237/2023, (Delhi HC Sept.20, 2023).

⁵ Information Technology (Intermediary Guidelines and Digital Media Ethics Code), 2021, Amendment Rules, 2026, Rule No. 2(w)(a).

For instance, imagine you're a renowned health influencer who has gained public trust over the years. A protein shake company takes advantage of your goodwill by making an Ad looking like you're promoting their product with the use of AI without your knowledge or consent; your followers buy this product, believing it was you in a fake advertisement. The legal remedy available to you will be to sue the company for defamation, ask for a John Doe (Ashok Kumar) injunction, and charge them with identity theft and cheating by impersonation under the IT Act, 2000, and relevant provisions of the BNS, 2023. While the Indian judiciary up to now has creatively applied existing Intellectual Property Laws to protect the victims, significant legislative gaps remain with the rapid advancement in the use of AI.

We need to understand why there is a need to protect our personal identity and information from AI exploitation, as it can be misused in such a way that damages reputation, bodily autonomy, and dignity of that person, which may even result in financial or commercial loss. There needs to be a dedicated legal framework, or amendments to existing laws, or mandated guidelines that could regulate the illegitimate use of AI in the creation of synthetic media that uses a person's identity. Much like the 'Safety and Ethical Guardrails' on AI models that prohibit it from processing prompts to clone personal features like body & vocal mannerisms, biometric data, and distinguishable elements without consent, and mandating intermediary liability for digital platforms to implement methods like 'Hashing' or 'digital watermarking' to verify and block re-uploads of harmful AI-generated videos.