



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.

DIGITAL DOPPELGANGER AND THE LAW: DEEPPFAKES AS A THREAT TO PRIVACY

~Anshika Singh



INTRODUCTION

With the advance of AI and its overwhelming use in various fields like- education, law, research, healthcare and finance it must also be kept in check. Its recurrent use prompts concern and also raises ethical issues related to surveillance and transparency. Deepfakes are a particularly significant tool for misinformation and digital imitation.

WHAT ARE DEEPPFAKES?

Deepfakes rely on Generative AI and Machine learning algorithms trained on massive set of data of a person's photos or voice recordings. The AI learns the person's facial expressions, vocal inflections, and mannerisms to flawlessly synthesize new, fabricated content. These generally include video, audio, or image, which is manipulated using Deep Learning (DL) algorithms that alters the original content with fake changes that look authentic. It is difficult to differentiate between an original image and a deepfake as these convincingly replicate a real person's likeness making them say or do what they never did. Alarming, 27%–50% of

people cannot distinguish deepfake-generated content from the real ones. This makes deepfakes an increasing threat in disinformation¹. According to a 2023 report by *DeepMedia*, over 5,00,000 videos and voice deepfakes were shared online. Deepfakes are the most significant example of misuse of AI, these are often used to extort, blackmail people. There exist various controversies regarding deepfakes-

- In 2024, a CEO was manipulated into approving a \$25.6 million transfer during an AI-generated video call. Businesses reported nearly \$450,000 in verified losses, contributing to total financial damages exceeding \$600,000².

OTHER MAJOR CONTROVERSIES- Beyond finance, deepfakes have also heavily deployed to corrupt political information around the globe, some other major examples are-

- ✧ The circulation of the **fabricated video of Ukrainian President, Volodymyr Zelensky**, appearing to tell his soldiers to lay down their arms and surrender the fight against Russia. "This is the first one we've seen that really got some legs, but I suspect it's the tip of the iceberg," said Hany Farid, a professor at the University of California, who is an expert in digital media forensics.³
- ✧ **GROK CONTROVERSY-** in early 2026 Grok faced legal scrutiny, for permitting mass generation of hyper-realistic, non-consensual explicit synthetic content. Users exploited this generative AI to create and distribute sexualized images of real individuals including public figures.
- ✧ Another major controversy in this aspect is **Baby Doll Instagram case**, in which a fake Instagram account was created with deepfakes of a girl with just one picture, the account was operated by an engineer for revenge, what started as harassment changed into a profit making account. This case highlights the depth of this issue that how deepfakes can change the whole scenario of social media operations, and how it can severely undermine the privacy of individuals.

¹ Christopher Doss, Tal Wolfson, Denise Kopecky, Valerie A, Lance Bush, *Deepfakes and scientific knowledge dissemination*, <https://dx.doi.org/10.1038/s41598-023-39944-3>

² Felipe Romero-Moreno, *Deepfake detection in generative AI: A legal framework proposal to protect human rights*, <https://www.sciencedirect.com/science/article/pii/S2212473X25000355>

³ Bobby Allyn, *Deepfake video of Zelenskyy could be 'tip of the iceberg' in info war, experts warn*, NPR, <https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia>

RIGHT TO PRIVACY- ITS ORIGIN AND SIGNIFICANCE

Section 21 includes within its ambit the Right to privacy guaranteed to every individual. Earlier, Right to Privacy was not a fundamental right; in fact the Supreme Court denied this right, in the case of *MP Sharma v. Satish Chandra*⁴ where the bench examined whether search and seizure powers violated a “right to privacy.” The Court’s answer was blunt: no such right existed under the Constitution.

The milestone came in *People’s Union for Civil Liberties (PUCL) v. Union of India*⁵—popularly known as the “telephone tapping case.” Here, the Court was asked whether the State could intercept calls without violating rights. It was held that unauthorised telephone tapping in fact infringed Article 21, and it laid down procedural safeguards, to prevent arbitrary and unnecessary encroachment upon right to privacy.

Finally, in *Justice K.S. Puttaswamy (Retd.) v. Union of India*⁶, a nine-judge bench settled the debate and unanimously held that privacy is inherent to life and personal liberty under Article 21. It defined privacy in three aspects: bodily privacy, decisional autonomy, and informational privacy. The judgment also recognised that in this digital era, protecting data privacy was crucial to preserving individual dignity.

HOW DEEPFAKES ENDANGERS THE RIGHT TO PRIVACY?

This misuse of AI, majorly deepfakes, poses a massive threat to India’s Constitutional values. The base of privacy is **consent**, using a person’s face or voice without their consent infringes their right to privacy. AI is a menace to Right to privacy on the grounds that:

1. **CONSENT WITHOUT CHOICE:** non-consensual use of one’s identity is a breach to his right to privacy.
2. **OPACITY:** also known as the black box problem which explains how the process by which data is processed is unknown to the use also poses as a great threat to the right

⁴ MP Sharma v. Satish Chandra, AIR 1954 SC 300

⁵ People’s Union for Civil Liberties v. Union of India, AIR 1997 SC 568

⁶ Justice K.S. Puttaswamy (Retd.) v. Union of India, AIR 2018 SC (SUPP) 1841

to privacy of the individuals. The users also vest in them the right to get explanation to know how their data is used.

3. **DATA HARVESTING:** data of the users is used commercially without their consent. Ai companies often scrape public sites to train their models.
4. **DISCRIMINATION AND ALGORITHMIC BIAS:** AI systems are only as fair as the data uploaded into them. For instance, *predictive policing tools* trained on biased crime data may irrationally target minority communities. Such outcomes collide with the constitutional promise of equality before the law under Article 14⁷.

LEGAL REGULATIONS AIMING TO PROTECT DATA:

Current Legal Regulations: In India, there is no proper statute which regulates the use of AI but there exists an Act which provides with some rules and regulations which are mandatory to be followed. The **Digital Personal Data Protection Act, 2023** is a comprehensive data protection Act. The DPDP law borrows from the EU's GDPR approach and extends coverage to all entities which process personal data. It also creates a set of rights for individuals whose personal data is processed. Further, it establishes a supervisory authority called the *Data Protection Board of India*.

ATTAINABLE REFORMS:

If privacy is to survive in the age of Artificial Intelligence, India's constitutional and legal framework must evolve. The reforms must recognize the justifiable use of AI, but must protect every individual's right to protect their information. Some possible reforms could be-

- An AI Charter
- Embedding privacy in basic design
- Mandatory Risk Assessment
- Algorithmic Transparency and Human Oversight
- Consent and Data Minimization
- Synthetic Content Regulation

⁷ Sonali Aggarwal, *ARTIFICIAL INTELLIGENCE AND THE RIGHT TO PRIVACY: A CONSTITUTIONAL CHALLENGE FOR INDIA*, Vol VII, Indian Journal of Law and Legal Research , <https://www.ijllr.com/post/artificial-intelligence-and-the-right-to-privacy-a-constitutional-challenge-for-india>