LEGAL AMENITY LAW JOURNAL – ISSN 3107-9148

Volume II Issue II March – April 2026

DEEPFAKES: LAW, SOCIETY & PSYCHOLOGY

By: - Ankita Mathur

3rd Year Law Student, JECRC University.

ABSTRACT

Deep fake technology, which uses artificial intelligence to create realistic fake videos, images, and audio, has quickly become a major issue in today's digital world. What began as a technical innovation is now widely accessible, allowing even ordinary users to create convincing fake content?

This paper explores deep fakes from multiple perspectives (including their impact on individuals, society, and the legal system. It highlights how deep fakes affect trust, spread misinformation, harm reputations, and create challenges for law enforcement, especially in India).

While the technology has useful applications in entertainment, education, and healthcare, its misuse is growing rapidly. This paper argues that addressing deep fakes requires a balanced and coordinated approach involving law, technology, platform regulation, and public awareness.

Keywords: Deep fakes, Artificial Intelligence, GAN, Misinformation, Reputational Harm, IT Act, DPDP Act, EU AI Act, Electoral Integrity, Platform Accountability.

INTRODUCTION

Deep fakes are AI-generated media that make it appear as though a person said or did something they never actually did. Over time, this technology has become easier to use and more widely available, making it both powerful and dangerous.

In the beginning, deep fake tools were limited to researchers and experts. Today, simple applications allow anyone to create highly realistic fake content within minutes. This shift has raised serious concerns about misuse in areas like politics, personal privacy, and financial fraud.

According to industry reports bright defense found that Deep fake fraud attempts have surged 2,137% in the last three years, and in 2024, a new deep fake attack was attempted every five minutes. [1]

And Thales 2026 Data Threat Report Finds 64% of Organizations in India Rank AI-Enabled Attacks as Top Data Security Risk.[2]

These are not abstract statistics. They represent destroyed reputations, manipulated elections, fraudulent financial transfers, and in documented cases, psychological trauma serious enough to require clinical intervention.

One of the most important issues is the breakdown of trust. Earlier, video and audio recordings were considered reliable forms of evidence. Now, people often question whether what they see online is real or fake. This creates confusion and weakens confidence in information systems. This paper traces the evolution of deep fake technology, examines the psychological and social damage.[3]

EVOLUTION OF DEEP FAKE TECHNOLOGY

Let's understand the evolution of deerflies through phases:

Phase 1 (2014):

The foundation was laid with the introduction of Generative Adversarial Networks (GANs) by Ian Good fellow in 2014. A GAN consists of two neural networks that compete with each other: The Generator, which creates synthetic content, and the Discriminator, which evaluates

[1] *Bright Defense, 150+ Deepfake Statistics (Mar. 2026), https://www.brightdefense.com/resources/deepfake-statistics/*

[2] *Thales Grp. & S&P Glob. 451 Rsch., Thales 2026 Data Threat Report (Feb. 25, 2026), https://www.businesswire.com/news/home/20260225890645*

[3] *Weaponizing reality: The evolution of deepfake technology | IBM https://share.google/QNDUMwmqGQg80ZRTu*

whether that content appears real. This process enables the creation of highly realistic artificial data.

Phase 2 (2017):

The term "deep fake" was first used by a Reddit user known as "deep fakes," who applied GAN-based techniques to create manipulated videos. This marked the beginning of widespread public awareness, although much of the early use was controversial.

Phase 3 (2018):

Deep fakes entered the mainstream with the release of accessible open-source tools such as DeepFaceLab. These tools significantly lowered the technical barrier, allowing non-experts to create realistic manipulated media.

Phase 4 (2023):

By 2023, the deep fake ecosystem expanded rapidly, with a significant increase in the development and availability of such tools. This growth further accelerated both legitimate applications and potential misuse.

PSYCHOLOGICAL IMPACT

Deep fakes have a significant impact on mental health and human behavior. One of the most noticeable effects is a growing distrust in media. People begin to doubt even genuine content, which creates uncertainty and anxiety. Victims of deep fakes often suffer serious emotional harm. Fake videos can damage a person's reputation, relationships, and career. In many cases, individuals experience stress, anxiety, depression, and even trauma.

In a world of advanced synthetic media, AI literacy isn't just about using AI tools (it's about surviving in an AI-mediated reality where seeing and hearing are no longer believing).[4] This reduces accountability and makes it harder to establish the truth.

And in the article The Psychological Impacts of Deep fakes: How Digital Manipulation Hurts People[5] How Deep fakes audio, video affect.

Deep fakes are no longer just technological curiosities, they're reshaping how people experience trust, safety, and even their own identities. As synthetic media spreads, its psychological and societal consequences are becoming impossible to ignore.

[4] *UNESCO, Deepfakes and Crisis: Knowing, https://www.unesco.org/en/articles/deepfakes-and-crisis-knowing*

[5] *Psychological Effects of Deepfakes https://share.google/GOp7ntf7NUeWL4qpC*

- Deep fakes can cause severe psychological harm, including anxiety, PTSD, and loss of personal agency for victims.
- 98% of deep fakes online are pornographic and primarily target women—making this a large-scale gender-based abuse issue.
- Societal trust is eroding as deep fakes fuel disinformation and create the "liar's dividend," where even real evidence is doubted.
- Governments are responding with stronger laws like the U.S. TAKE IT DOWN Act and the EU AI Act, and victim support programs are expanding.
- Deep fake detection, watermarking, and authenticity standards (like C2PA) are critical for restoring digital trust.

SOCIAL IMPACT

Social media platforms have played a central role in the rapid proliferation of deep fake content. Their instantaneous dissemination mechanisms, algorithmic amplification, and large user bases make them particularly vulnerable to the spread of manipulated audio-visual material. Because content on such platforms is frequently consumed and shared without verification, deep fakes can achieve viral circulation within a very short period.

This concern is further intensified by the lack of public awareness regarding synthetic media. A study conducted by iProov found that in its global survey, approximately 71% of respondents did not know what a deep fake was, with less than one-third of consumers reporting familiarity with the concept. Such findings highlight the ease with which misinformation may spread through digital platforms and the difficulty ordinary users face in identifying manipulated content.[6]

Social media platforms play a major role in spreading deep fakes. Their algorithms are designed to promote engaging content, which often includes sensational or emotional material. This allows fake content to spread rapidly.

[6] *Deepfakes and Their Impact on Society | CPI OpenFox https://share.google/P9V0ygqzUKvI2uhAK*

Deep fakes also disrupted political landscapes by showing political figures saying or doing things they never did. One famous example of this involves

Ukrainian President Volodymyr Zelenskiy in a deep fake video asking his army to cease fighting. This not only undermines the trust in political leaders but also has the potential to change public opinion and influence elections. study conducted by the University of Baltimore and Cybersecurity firm CHEQ, found that in 2020, fake news cost the global economy $78 billion.[7]

Recently on 15th April 2026 Two RJD spokespersons, Priyanka Bharti and Kanchana Yadav, were booked by police for sharing a misleading video falsely linked to the Noida workers' protest.

The video actually showed an unrelated incident from Madhya Pradesh, and authorities said it was shared to spread rumors and incite tension during the protests.[8]

Through this Fake videos or audio clips circulate misinformation between society. This creates serious risks for democratic systems. It can also affect businesses, healthcare, and other institutions by spreading false information and damaging trust.

LEGAL FRAMEWORK

Legal Framework (India & Comparative)

India presently does not possess a dedicated and comprehensive statute explicitly addressing deep fake technology. The applicable legal framework is inherently constructed from provisions enacted for various purposes, resulting in a fragmented, reactive, and insufficient coverage that fails to match the scale and sophistication of the issue.

The European Union has taken a significant step in addressing the risks posed by deep fakes and AI-generated misinformation through the enactment of the European Union AI Act.

This legislation establishes a comprehensive, risk-based framework that classifies artificial intelligence systems according to their potential impact and imposes corresponding regulatory obligations. Notably, the Act introduces transparency requirements mandating that users be

[7] *Deepfakes and Their Impact on Society | CPI OpenFox https://share.google/uu3etfHk3hcQVsQer*
[8] *Noida workers' protests: Two RJD spokespersons booked for sharing 'misleading' video, inciting tension - The Hindu https://share.google/egIcK0aMaY8fV9Cph*

informed when interacting with AI-generated content, particularly where there is a risk of deception or impersonation. It further imposes strict compliance obligations on both developers and deplorers of AI systems, supported by substantial financial penalties for non-compliance, which may extend up to €35 million or 7% of global annual turnover. However, despite its innovative approach, concerns remain regarding the effectiveness of such regulatory measures, particularly in light of rapid technological advancements, enforcement challenges across jurisdictions, and the limitations of post-facto penalties in preventing the creation and dissemination of harmful deep fake content. [9]

IT laws

The Information Technology Act, 2000 (IT Act) contains the most directly applicable existing provisions. Section 66C targets identity theft through fraudulent impersonation using any communication device or computer resource, carrying imprisonment of up to three years and a fine up to ₹1 lakh. Section 66D addresses cheating by impersonation through computer resources with identical penalties. Section 66E addresses the capture, publication, or transmission of images depicting private areas without consent, carrying imprisonment up to three years and a minimum fine of ₹2 lakhs. Sections 67, 67A, and 67B prohibit obscene, sexually explicit, and child sexual abuse material respectively. [10]

The Digital Personal Data Protection Act, 2023 (DPDP Act), while not yet fully implemented, provides a structural framework relevant to deep fake regulation. As argued by scholars at Jindal Global Law School (2026), deep fakes constitute processing of personal data under the Act. Data fiduciaries creating or circulating deep fakes must obtain explicit consent from data principals; failure to do so constitutes unlawful processing. The Act also grants data principals the right to correction and erasure, which could serve as a mechanism for victims to demand removal of fabricated content. [11]

[9] *Deepfake, Deep Trouble: The European AI Act and the Fight Against AI-Generated Misinformation, Colum. J. Eur. L. (2024), https://cjel.law.columbia.edu/preliminary-reference/2024/deepfake-deep-trouble-the-european-ai-act-and-the-fight-against-ai-generated-misinformation/*

[10] *Khurana & Khurana, Deepfake Regulation India 2025: MeitY's Comprehensive IT Rules Amendment (Dec. 2025), https://www.khuranaandkhurana.com/deepfake-regulation-india-2025-meity-s-comprehensive-it-rules-amendment*

[11] *Paarth Naithani, Regulating Deepfakes under India's Digital Personal Data Protection Act, 2023, Econ. & Pol. Wkly. (2026), https://www.epw.in/engage/article/regulating-deepfakes-under-indias-digital-personal*

Privacy & personality rights

The Supreme Court's landmark decision in Justice K.S. Puttaswamy v. Union of India (2017) established the right to privacy as a fundamental right under Article 21 of the Constitution.

The judgment explicitly holds that an individual's right to privacy encompasses control over the dissemination of personal information, including one's image and likeness.

Courts have applied this reasoning to hold that unauthorized deep fake usage violates the constitutional right to privacy regardless of whether the specific conduct falls within an enumerated statutory prohibition.[12]

Defamation

Deep fake videos that falsely depict real individuals engaging in criminal conduct, making offensive statements, or participating in sexual activity are straightforwardly defamatory in their effect. However, as noted in the Springer Nature (2024) analysis, successfully proving that a deep fake was created and distributed with defamatory intent (and tracing that creation to an identifiable person) presents evidentiary challenges that conventional defamation litigation was not designed to address. The landmark Subramanian Swamy v. Union of India (2016) decision, which upheld the validity of criminal defamation laws in the digital context, provides important precedent for deepfake-mediated reputational harm. [13]

CHALLENGES

India does not currently have a specific law that directly addresses deep fakes. Instead, existing laws such as the Information Technology Act and data protection laws are used to deal with related issues like identity theft, fraud, and privacy violations. Courts have recognized that using someone's image or identity without permission can violate their rights. Other countries have started developing specific laws to regulate AI-generated content. These laws focus on transparency, accountability, and protection of individual rights.

[12] *Regulating Deepfakes: An Indian Perspective, J. Strategic Sec. (2024), https://digitalcommons.usf.edu/cgi/viewcontent.cgi?article=2245&context=jss*

[13] *Deepfakes and the Law: Fighting AI Fakery and Protecting Image Rights in India, Lawful Legal (2025), https://lawfullegal.in/deepfakes-and-the-law-fighting-ai-fakery-and-protecting-image-rights-in-india/*

One of the biggest challenges in dealing with deep fakes is identifying the person responsible for creating them. Many creators operate anonymously or from different countries, making enforcement difficult.

Another major issue is speed. Deep fakes spread very quickly online, while legal processes take time. By the time action is taken, the damage is often already done. There is also a lack of technical infrastructure and trained personnel to investigate such cases effectively.

Recent cases

Akshay Hari Om Bhatia v. John Doe -The Bombay High Court, in Akshay Hari Om Bhatia v. John Doe, held that AI-generated deepfake content violating a person's image, voice, and identity infringes personality and fundamental rights under Article 21.

The Court granted urgent ex parte relief and ordered immediate takedown of such content, recognizing the serious risks posed by realistic deep fakes to both individual dignity and public safety.[14]

Asha Bhosle and voice cloning law in India

The Asha Bhosle case expanded the conversation beyond face manipulation. It focused on voice cloning. The Bombay High Court acknowledged that a voice is not just sound. It is identity. It is legacy. It is personality. This became a defining moment for voice cloning law in India. It established that AI replication of someone's vocals without permission can violate personality rights and dignity.

The law is adapting to technology. Slowly. But firmly.

Abhishek Bachchan, Shilpa Shetty, Vivek Oberoi - expanding the shield

The Delhi High Court granted relief to Abhishek Bachchan against unauthorized exploitation of his name and AI-generated images. The Bombay High Court extended protection to Shilpa

[14] *Bombay HC condemns Akshay Kumar deepfake video | SCC Times https://share.google/obOu3PvK6ZIYmNWYO*

Shetty against multiple defendants misusing her identity. Vivek Oberoi secured protection against AI-driven deep fakes and unauthorized merchandise.[15]

These cases reinforce a pattern. Courts are not treating personality rights as abstract theory anymore. They are treating them as enforceable legal interests. Search terms like celebrity personality rights India, right of publicity in India, and unauthorized use of name image voice India are rising for a reason. People are connecting the dots

RECOMMENDATIONS

Based on the foregoing analysis, this paper proposes the following legal reform priorities:

For India:

- **Enact dedicated deepfake legislation** establishing clear definitions, explicit consent requirements for likeness usage, specified categories of prohibited deepfake conduct, proportionate criminal and civil penalties, and mandatory remedial mechanisms.
- **Implement the DPDP Act fully** and issue rules explicitly addressing deepfake-specific data processing, including biometric data protections applicable to AI training datasets.
- **Enact statutory personality rights legislation** moving beyond judicial interpretation to provide clear, accessible statutory protection for every individual's control over their name, image, voice, and likeness.
- **Establish an Inter-Ministerial Deepfake Coordination Body** comprising MeitY, the Ministry of Law and Justice, CERT-In, the National Cyber Crime Coordination Centre, the Election Commission, and independent civil society and technical experts.
- **Invest in cyber-forensic capacity** through dedicated training of law enforcement units, partnerships with academic forensic research programs, and equipping prosecutors with technical expertise.

Globally:

- **Develop international treaty standards** on deepfake definition, disclosure requirements, and mutual legal assistance for enforcement against transnational deepfake operations.

[15] *Deepfake Law in India - Akshay Kumar, Anil Kapoor, Suniel Shetty Cases https://share.google/qcm0MMQVvcRc8tpxk*

- **Mandate C2PA provenance standards** for generative AI platforms as a condition of market access, creating a global baseline for content authentication.
- **Support media literacy education** as a population-level defense, recognizing that technological and legal tools alone cannot protect democratic societies without widespread critical media consumption skills.

CONCLUSION

Deepfakes represent a serious challenge in the modern digital world. They affect trust, privacy, and the functioning of society as a whole.

While the technology itself is not harmful, its misuse creates significant risks. Addressing these risks requires a balanced approach that combines legal measures, technological solutions, and public awareness.

If timely action is not taken, the impact of deepfakes will continue to grow, making it increasingly difficult to distinguish between reality and manipulation.