# The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2024

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




## Deepfake: Intellectual Property and AI – A Tangled Web!

### 1. INTRODUCTION

The term "Deepfake" originated in 2017 on Reddit, where users began superimposing celebrities' faces onto different individuals, particularly in adult content. The term “deepfake” comes from the combination of “deep machine learning” and “fake.”[1]

The advent of generative Artificial Intelligence (AI) and deepfake technology marks a new era in intellectual property law, presenting unprecedented challenges and opportunities. As these technologies evolve, their creations blur the lines between reality and fiction, escalating the risk of consumer deception and diluting brand values.[2]

In India, Deepfakes have become synonymous with Rashmika Mandanna. On November 7, 2023, a deepfake video went viral online, showing her entering an elevator in a black yoga suit. However, it was later discovered that the original video featured social media influencer Zara Patel that was altered to look like Rashmika Mandanna using digital manipulation.

### 2. HOW DOES IT ALL WORK?

Deepfakes are made using deep learning algorithms. Deep learning is an AI function that mimics the workings of the human brain in processing data and so is able to learn without human supervision, as it learns by example. More specifically, synthetic media and deepfakes rely on

[1] Vejay Lalla, Adine Mitrani and Zach Harned, *Artificial intelligence: deepfakes in the entertainment industry*, WIPO MAGAZINE, (2022), Artificial intelligence: deepfakes in the entertainment industry (wipo.int)

[2] Alexis Kang, *Fake it ‘til You Make Law: The AI Identity Crisis*, J. OF TECH & INTELLECTUAL PROPERTY, (2024), Fake it ‘til You Make Law: The AI Identity Crisis - Journal of Technology and Intellectual Property (northwestern.edu)

Generative Adversarial Networks (GANs) and involve two deep neural networks competing to produce the most high-quality fakes. The network is made up of three components:

a) real-world data;

b) a discriminator; and

c) a generator.

The discriminator network is trained using true, real-world, data and it assesses whether the generator is producing real or fake content. The generator typically creates text, images, or video. It begins with random data, and, as the name suggests, it generates progressively better samples, to convince the discriminator that the sample is genuine real-world data.[3]

## 3. THE IP PERSONA!

The ascent of generative deepfake technology casts new challenges for IP Laws. Section 51 of the Indian Copyright Act of 1957 protects copyright owners from unauthorized use of their works, allowing them to pursue legal action. Furthermore, Section 52 of the Copyright Act of 1957 makes a clear distinction between legitimate and illegitimate users of protected works.[4] Deepfakes are not included in this list, making it easier to hold the creator liable.

In addition, Section 57(1)(b) of the Copyright Act of 1957 protects both the right of integrity and paternity.[5] Copyrighted works are protected against distortion, mutilation, and modification. Moral rights protect the creator's reputation and allow for attribution of their work.[6] The Berne Convention as required by Article 6bis, which states that moral rights must apply to all works.[7]

---

[3] Alex Walker, *Deepfakes and legal implications: Seeing is not believing*, CLIFORD CHANCE WEBSITE, (2020), Deepfakes and legal implications: Seeing is not believing (cliffordchance.com)

[4] §52,The Copyright Act, 1957, No. 14, Acts of Parliament, 1957 (India).

[5] Id. at §57.

[6] Betsy Rosenblatt, Moral Rights Basics, HARVARD UNIVERSITY (Jul. 23, 2020, 11:47 PM), https://cyber.harvard.edu/property/library/moralprimer.html#:~:text=In%20the%20United%20States%2C%20the,of%20who%20owns%20the%20work.

[7] Berne Convention for the Protection of Literary and Artistic Works, Sept. 9, 1886, as revised at Paris on July 24, 1971 and amended in 1979, S. Treaty Doc. No. 99-27 (1986) .

Likewise, the author has the right to create derivative works under Section 14 of the Copyright Act of 1957.[8] Sections 55[9] and 63[10] impose civil and criminal liability for violating exclusive rights. The existence of these provisions also makes it easier to impose liability on intermediaries as a result of the current legal position following Myspace Inc. v. Super Cassettes Industries Ltd[11] and Section 79 of the Information Technology Act, 2000,[12] which exempts online intermediaries from liability for any third-party information. While Rule 7 of the IT Rules allows aggrieved individuals to take platforms to court under IPC provisions.

In the IT Act 2000, Section 66 (computer-related offences) is punishable by imprisonment for three years, a fine of up to five lakh rupees, or both. S. 66C (Punishment for identity theft) is punishable by imprisonment up to three years and a fine of one lakh rupees. S. 66D penalizes cheating by personation using computer resources with up to three years imprisonment and/or a fine of ₹1 lakh, while S. 66E penalizes privacy violations with up to three years in prison or a fine of ₹2 lakh. [13]

Sections 67, 67A, and 67B of the IT Act 2000 specifically prohibit and punish publishing or transmitting obscene material containing sexually explicit acts and children depicted in the same in any electronic form.

The Ministry of Electronics and IT (MeitY) recently took a proactive stance to address the growing concerns about deepfake content on social media platforms. In the draft of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022 12,

Rule 3(1)(b)(vii), This Rule requires social media intermediaries to ensure that their platform's users do not host content that impersonates another person.

[8] §14.The Copyright Act, 1957, No. 14, Acts of Parliament, 1957 (India).
[9] Id. at §55.
[10] Id. at §63.
[11] Myspace Inc. v. Super Cassettes Industries Ltd, 2011 (48) PTC 49 (Del) (India).
[12] §79,The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000 (India)
[13] Harshvardhan Mudgal, *The deepfake dilemma: Detection and decree*, Bar and Bench Website, (2023), The deepfake dilemma: Detection and decree (barandbench.com)

Rule 3(2)(b): Such content must be removed within 24 hours of receiving a complaint.[14]

## 4. LAWSUITS THAT PAVED THE WAY AGAINST DEEPFAKES – INDIA[15]

In the case, Anil Kapoor v. Simply Life India and Ors[16], the Delhi High Court granted protection to Mr. Anil Kapoor's individual persona and personal attributes against misuse, specifically through AI (Artificial Intelligence) tools for creating deepfakes. The Court issued an ex-parte injunction, effectively prohibiting sixteen (16) entities from using the actor's name, likeness, image, and technological tools such as AI for financial gain or commercial purposes**.**

Similarly, in the case Amitabh Bachchan v. Rajat Negi and Ors[17], the legendary actor was granted an ad interim in rem injunction against the unauthorized use of his personality rights and personal attributes such as voice, name, image, and likeness for commercial purposes.

## 5. MITIGATION STRATERGY.

a) **Learning from Other Countries**: Deepfakes have three stages, creation, dissemination, and detection. AI regulation can be used to reduce the number of illegal or nonconsensual deepfakes.

*The European Union's Digital Services Act (DSA*) went into effect in November 2022, enhancing monitoring of online platforms for harmful content, such as deepfakes.

*Singapore* in 2019, passed the Protection from Online Falsehoods and Manipulation Act (POFMA), which allows the government to remove harmful content, including deepfakes.

[14] The Information Technology (Intermediaries Guidelines and Digital Media Ethics Code) Amendment Rules 2022, https://www.meity.gov.in/writereaddata/files/Draft_Intermediary_Amendment_24122022. pdf.
[15] Vikrant Rana , Anuradha Gandhi and Rachita Thakur, *India: Deepfakes And Breach Of Personal Data – A Bigger Picture*, (2023), S.S. Rana & Co. Advocate Deepfakes And Breach Of Personal Data – A Bigger Picture - Social Media - India (mondaq.com)
[16] CS(COMM) 652/2023 and I.A. 18237/2023-18243/2023
[17] 2022 SCC OnLine Del 4110.

*South Korea's Deepfake Prohibition Act*, enacted in July 2020, criminalizes the creation and distribution of harmful deepfakes, punishable by five years in prison or a fine of 50 million won.

b) **Watermarking and authentication:** They serve a variety of purposes by revealing the content's origin and ownership. Furthermore, watermarks promote accountability by providing proof of the original creator's rights, making it easier to enforce copyright and intellectual property protections for AI-generated content.

**c) Foster International Collaboration**

Given the internet's global nature and the ease with which deepfake content can cross borders, international cooperation is essential. Nations must collaborate to create consistent legal frameworks, share detection technologies, and coordinate efforts to effectively combat this evolving threat.

*For example,* The AI Safety Summit 2023 that took place at Bletchley Park in Buckinghamshire. The Bletchley Declaration, resulting from the collective agreement of 29 countries, including India, is a step toward creating a more rigorous environment for AI development and deployment.