The Evolution of Deepfake Laws: Adapting Copyright and Data Privacy Regulations to Emerging Threats

[1]Priyanka Mangaraj, [2]Malini Venugopal

Assistant Professor
School of Law
Presidency University, Bangalore.

Abstract- **Artificial intelligence (AI) has become a focal point in numerous discussions and developments. With the rapid increase in AI-based innovations, there is a notable absence of extensive public policy discussion on the intersection of AI and Intellectual Property Rights in India. 'Deep fakes' is a contentious AI innovation that requires a multi-faceted approach. Deep fakes are commercially used to assist the artists to spread their work to a broader target audience, as well as they could also become a part in infringing one's privacy on social media. The term 'deep fake' is not a novel term in India however, they do introduce some complexities that should be considered by the contracting parties. In the recent times, the use of deep fakes in morphing photos without consent leading to privacy infringement has added a new layer of complexity. However, on the positive aspect, deep fake technology has provided a livelihood to many actors who requires copyright protection for their skill and labour. In countries like United States, China, Singapore, the legal landscape of deep fakes is rapidly adapting with the current challenges, but India does not have specific provisions to handle the complexities of deep fakes. The vital question is whether this technology will strengthen or weaken intellectual rights of the original creators and what would be the impact on the moral rights of copyrighted work of celebrities. This paper will focus on the adequacy of the existing Indian laws for safeguarding deep fakes under fair use of copyright work and data privacy laws.**

Keywords: **AI, deepfakes, fair use, data privacy**

INTRODUCTION:

Artificial intelligence (AI) has revolutionized our lives in ways that were previously unthinkable. A few decades ago, the idea that a computer programme might duplicate human intellect was just science fiction. In contrast, artificial intelligence is now vital to human existence in many respects, most notably in e-commerce, finance, education, healthcare, marketing, agriculture, and industry. AI has rapidly evolved into an accelerating trend that is changing many facets of society, including the way information is created, disseminated, and consumed. As AI technologies advance like deep learning, new techniques have emerged to synthesize highly realistic fake media known as deepfakes. They present numerous possibilities for technological advancements and challenges that should be carefully evaluated especially when it involves Intellectual Property Rights (IPR) and Data Protection Laws. Even if deepfakes have some usefulness, there are serious concerns regarding how to amend legal definitions and frameworks to account for this new problem given their potential for misuse. Deepfakes push the boundaries of trademark and copyright law by using AI systems to mimic human identities and artistic creations independently. The unauthorized use of an individual's likeness and voice in deepfakes also creates tension with privacy rights. Thus, the IPR and data protection laws about deepfake technology are the primary focus of this paper.

Evolution of Deepfake Technology

Deepfake is a relatively new concept, yet several versions of deepfakes existed before the invention of artificial intelligence, such as Photoshop and face swap. The uniqueness of the results of deepfakes is the single factor that sets these methods apart. Unlike Photoshop and face swap procedures, deepfake makes it virtually hard to discern whether the media created is real or fake. The terms "Deep Learning" and "Fake" are combined to create Deepfake. Deepfakes are generated using artificial intelligence technology, namely machine learning techniques, as may be inferred from the combination.[1] The most used AI technologies to create deepfake content are Generative Adversarial Networks (GAN)

[1] Çolak. B., (2021, January 19), *Legal Issues of Deepfakes*, Institute for Internet & the Just Society,

https://www.internetjustsociety.org/legal-issues-of-deepfakes and Variational Auto-Encoders (VAE). It is a swapping method where original multimedia information—such as photos, films, and audio files—is placed over preexisting content. Deepfakes provide flawless speech replication in addition to the remarkably realistic recreation of facial and/or bodily features and motions.[2] An algorithm examines source videos or photographs of a target individual to gather information up on their speech patterns, mannerisms, and facial expressions before producing a deepfake video. By using this "source data," the AI system is trained to create a persona that it may use to create new audio and video content that features them. The subsequently created deepfake might realistically portray the target person speaking or doing things they have never done before.

The term “deepfakes” was first coined in late 2017 when a Reddit user with the pseudonym “deepfakes” shared doctored pornographic videos on the site. He performed this by superimposing the faces of celebrities on the bodies of pornographic performers using Google’s open-source, deep-learning technology. The codes contained in most deepfakes discovered in the open today are derived from this original code.[3] An open-source deepfake algorithm called FakeApp launched in 2017, allowing anyone to create deepfakes on consumer GPUs. This democratized production and kicked off the current deepfakes era. Large datasets, GPU-enabled consumer computer power, and Generative Adversarial Networks like StyleGAN, BigGAN, etc. all contributed to significant advances in deepfake quality during 2018 and 2020.

In the modern world, deepfake is employed in various streams, ranging from entertainment to the health industry. One of the primary disadvantages of deepfakes is that they are frequently used to create revenge porn, which is used to harass women and celebrities. Additionally, there are several concerns associated with this technology, including identity theft, fraud, political manipulation, fabrication of false evidence, and cybersecurity issues. However, deepfake technology has a myriad of positive implications in the fields of healthcare, fashion, movies, education, and entertainment. For legal and regulatory institutions, the development of deepfake technology poses complex challenges.

Deepfake Technology in India

Artificial intelligence (AI) and machine learning algorithms are the driving forces behind deepfake technology, which is transforming several countries, including India. India has witnessed a rise in the use of deepfakes from entertainment to misinformation as they become more widely available. Lately, there have been numerous instances of deepfake technology being used in India, prompting authorities to adopt a more proactive stance in addressing this issue. This technology frequently targets Bollywood actors and actresses. In 2023, there were multiple reported incidents, including a manipulated video of actress Rashmika Mandanna circulating on social media. That altered video featured her face superimposed onto a British-Indian influencer’s video. After this event, fake images of actresses Katrina Kaif, Kajol, and Alia Bhatt began to spread similarly. The alteration of video footage featuring actor Amitabh Bachchan is another instance of the inappropriate use of this technology. Nevertheless, the film industry has significantly profited from the use of this technology.

Deepfakes can potentially be used to spread political misinformation and sway elections, which raises concerns. The Prime Minister, Narendra Modi, recently warned about the issue, mentioning a deepfake video of himself participating in garba that he had come across. One of the first instances of deepfakes being used in political campaigning was in 2020, during which the videos of Manoj Tiwari, the leader of the Bharatiya Janata Party, were shared across social media before the Delhi Elections. This video was created by combining one of his previous videos with another one in which he discussed an entirely unrelated topic. Later in 2021, a fake video purporting to show Congress leader Rahul Gandhi calling Modi supporters “poor” went viral just before the key state elections. In addition to identity and political risks, there have been other documented problems with deepfakes in India, such as calls from scammers pretending to be business executives or government officials to get personal information and commit financial fraud.

Just like a coin, there are both sides to this deepfake AI technology. Nobody is concentrating on the advantages of this revolutionary technology that the world has never seen before, while the bulk of us—including the media—are working to promote the terror of deepfakes. Because of AI, almost every industry in the world is advancing. Positive developments, mostly in the form of films and commercials, have been observed, particularly in India. Deepfakes have so far been used in real-world applications, for instance, Salman Khan's dual part in the Pepsi commercial and Shah

[2] Tammaro. M., (2022, August 30), Deepfake: the fine line between fiction and reality, Clifford Chance, https://www.cliffordchance.com/expertise/services/intellectual-property/global-ip-updates/2022/q4/deepfake-the-fine-line-between-fiction-and-reality.html

[3] Adee. S., (2020, April 29), What Are Deepfakes and How Are They Created? Deepfake technologies: What they are, what they do, and how they’re made, IEEE Spectrum, https://spectrum.ieee.org/what-is-deepfake

Rukh Khan's My Ad campaign, a customized Cadbury advertisement, where anybody may deepfake their face to appear to be starring alongside the Bollywood star. This AI technology can also enhance the functionality of autonomous and self-driving cars. Deepfake finds applications in the healthcare industry in addition to entertainment, film, and automotive industries. In 2018 research, the MGH & BWH Centre for Clinical Data Science, NVIDIA, and the Mayo Clinic employed deepfake to augment uncommon anomaly photos with synthetic ones, increasing the accuracy of AI diagnostics.[4] Another positive impact was that a non-governmental organization produced a deepfake video featuring a deceased father preaching against tobacco use in an attempt to discourage his kid from doing drugs. This effectively drove societal transformation through AI.

Deepfakes and AI-related crimes are not specifically covered by any laws in India, although there are provisions under several statutes that may provide both criminal and civil remedies. India regulates deepfake technology through various legal instruments mainly IT Act, 2000[5] and IT Rules[6]. IT Act provides the provisions for privacy infringement and its punishments whereas IT Rules are directions to the intermediaries. Under the IT Rules, social media platforms must promptly remove artificially morphed images of people upon notification and are forbidden from hosting any content that impersonates another person. The safe harbor guarantee, which shields social media firms from legal responsibility for user-shared information from third parties, might be lost if they fail to remove such content. For cybercrimes related to deepfakes, the Indian Penal Code, 1860[7] (IPC) provisions may also be invoked. In addition, the use of any copyrighted picture or video in the creation of deepfakes may give rise to legal action under the Copyright Act of 1957.[8] The recently passed Data Protection Act, 2023[9] is an addition to this list, which safeguards individuals' rights and personal information.

Legal Protection in India for Deep Fakes Technology:

In India, there is no specific regulation directly addressing deep fakes. However, to combat the misuse of deepfake technology, existing laws offer various causes of action that may apply or be extended for applicability. Here's a summary of pertinent provisions:

1. Right to Privacy:

The fundamental right to privacy, derived from Article 21 of the Constitution of India, 1950, encompasses 'informational privacy.' In Justice K. S. Puttaswamy v. Union of India,[10] the Supreme Court recognized that individuals have the right to control the dissemination of personal material, including digital privacy. Therefore, utilizing personal information in deepfake videos without consent violates the fundamental right to privacy.[11]

Additionally, Section 66E of the Information Technology Act, 2000 (IT Act) imposes penalties for privacy violations. If a person intentionally captures, publishes, or transmits an image of a private area without consent, they may face imprisonment for up to three years, a fine not exceeding two lakh rupees, or both.

2. Information and Technology Act 2000 -

[4] Shin, H.-C., Tenenholtz, N. A., Rogers, J. K., Schwarz, C. G., Senjem, M. L., Gunter, J. L., Andriole, K. P., & Michalski, M. (2018). Medical Image Synthesis for Data Augmentation and Anonymization using Generative Adversarial Networks. https://doi.org/10.48550/arxiv.1807.10225

[5] The Information and Technology Act, 2000 (Act No. 21 of 2000)

[6] The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, G.S,R. 139(E), published in the Gazette of India.

[7] The Indian Penal Code, 1860 (Act No. 45 of 1860)

[8] The Copyright Act, 1957 (Act No.14 of 1957)

[9] The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023)

[10] (2017) 10 S.C.C. 1

[11] Justice K. S. Puttaswamy v. Union of India, (2017) 10 S.C.C. 1

The misuse of deep fakes falls under computer-related offenses according to the IT Act, 2000. Section 67 of Act[12] penalizes the publication or transmission of obscene material in electronic form, while Section 67A[13] addresses the publishing or transmitting of material containing sexually explicit acts. Moreover, Section 67B[14] punishes the publication or transmission of material depicting children in sexually explicit acts.

If a deep fake video involves fraudulent use of electronic signatures, passwords, or unique identification features, the accused can be charged with identity theft under Section 66C[15] of the IT Act. Additionally, cheating by personation using computer resources or communication devices is punishable under Section 66D of the IT Act.[16]

Furthermore, the Central Government holds the authority to direct intermediaries to block public access to any deep fake content generated, transmitted, received, stored, or hosted in computer resources if deemed necessary for the interests of sovereignty, integrity, defense, security, friendly relations, or public order, or to prevent incitement to cognizable offenses related to these concerns.

3. Defamation -

In India, an individual can face defamation liability under both civil and criminal law. In civil defamation, damages are awarded if defamation is proven in a legal action. Criminal defamation encompasses visible representations causing or likely to cause harm to a person's reputation, with punishment specified in Section 500 of the Indian Penal Code, including imprisonment for up to two years or a fine, or both. However, these provisions may not fully address the diverse forms of deep fakes.[17]

Previously, cyber defamation was addressed under Section 66A of the IT Act, which penalized sending offensive or menacing information via computer resources. However, the Supreme Court, in Shreya Singhal v. Union of India, struck down this provision.[18]

4. Criminal Liability -

Deepfake videos, essentially altered versions of original content, can potentially constitute forgery. Committing forgery with the intent that the forged electronic record harms the reputation of any party, or knowing that it's likely to be used for such purpose, is punishable under Section 468 of the Indian Penal Code. The penalty may include imprisonment for up to three years and a fine.[19]

If a deep fake aims to generate hatred, contempt, or disaffection towards the lawful Government in India, it falls under the offense of sedition, as per Section 124 of the IPC.[20]

Additionally, if a person in a deep fake video is threatened with harm to their reputation or property, or if an interested person is targeted with the intent to cause alarm or induce illegal actions, it constitutes the offense of criminal intimidation.[21] Section 506 of the Indian Penal Code provides punishment for this offense, encompassing the use of photos or videos to threaten or intimidate any person, their property, or reputation.

Furthermore, depending on the potential consequences of the deep fake content, the accused may face charges for intentional insult with the intent to provoke a breach of peace, promoting enmity between different groups based on

[12] Section 67, Information and Technology Act, 2000

[13] Section 67A, Information and Technology Act, 2000

[14] Section 67B, Information and Technology Act, 2000

[15] Section 66C, Information and Technology Act, 2000

[16] Section 66D, Information and Technology Act, 2000

[17] Section 500, Indian Penal Code, 1860

[18] A.I.R. 2015 S.C. 1523

[19] Section 469, Indian Penal Code, 1860

[20] Section 124, Indian Penal Code, 1860

[21] Section 503, Indian Penal Code, 1860

factors like religion, race, place of birth, residence, language, etc., engaging in acts prejudicial to the maintenance of harmony, or committing deliberate and malicious acts intended to outrage religious feelings of any class by insulting its religion or religious beliefs.[22]

Legal Stand of Various Countries for Deep Fakes:

Deepfakes leverage machine learning to interchange faces, attributing one person's behavior to another through digital impersonation. This AI technique fabricates events that never occurred, fundamentally reshaping reality. Generative Adversarial Networks (GANs) are commonly employed in deep fake creation, where two algorithms compete to generate authentic-looking synthetic media.[23] Despite malicious applications, such as using deepfakes for revenge porn or manipulating political campaigns, the technology presents opportunities for legitimate uses, such as crafting entertainment parodies and resurrecting deceased actors in the film industry.[24]

Current legislative developments regarding deep fakes often overlook the potential impact on copyrights, possibly stemming from the misconception that existing copyright protection can effectively combat deepfake-related infringements. However, copyright laws in various jurisdictions don't uniformly safeguard rights when violated by deep fakes. The effectiveness of doctrines like "fair use" in the US's Digital Millennium Copyright Act of 1998[25] and "fair dealing" in the Indian Copyright Act of 1957[26] and the United Kingdom Copyright, Designs, and Patent Act of 1988[27] differs, reflecting distinct approaches in these legal frameworks to address challenges arising from this disruptive technology.

Deep fakes under the Indian Copyright Act 1957 -

In India, Section 52 of the Indian Copyright Act, 1957, addresses excluded works under the doctrine of fair dealing.[28] Unlike the U.S., fair dealing in India is an exception to copyright infringement, with a specific list of non-infringing acts. While criticized for its rigidity, this approach proves useful in combating malicious deep fake technology as such usage doesn't align with the listed acts. However, the provision may not protect legitimate applications of deepfake technology.

Indian courts are incorporating the concept of transformative use, particularly regarding 'review' in Section 52(1)(a)(ii) of the Act, as seen in the University of Oxford and Ors. v. Narendra Publishing and Ors.[29] This includes the incorporation of fair use into fair dealing to protect certain works beneficial to society. Notably, existing precedents on transformative use have focused on guidebooks within the literary works category and may not directly apply to deep fakes.[30]

[22] Section 295A, Indian Penal Code, 1860

[23] Karen Hao, 'Inside the world of AI that forges beautiful art and terrifying deepfakes' (MIT Technology Review, 1 December 2018) <https://www.technologyreview.com/2018/12/01/138847/inside-the-world-of-ai-that-forges-beautiful-art-and-terrifying-deepfakes/>

[24] Robin Pomeroy, 'This iconic film star will star in a new movie – from beyond the grave' (World Economic Forum, 8 November 2019) <https://www.weforum.org/agenda/2019/11/james-dean-cgi-deepfakes/>

[25] The Digital Millennium Copyright Act 17 U.S.C. §107 (1998) (USA)

[26] The Copyright Act 1957 No.14 Acts of Parliament 1957 (ICA 1957) (India)

[27] Copyright, Designs and Patent Act 1988 (CDPA 1988) (UK)

[28] ICA 1957, s 52

[29] *University of Oxford v Narendra Publishing House, ILR* (2009) 2 Del 221

[30] *University of Cambridge v B.D. Bhandari* (2011) SCC OnLine Del 3215; *Saregama India Limited v Balaji Motion Pictures Limited and Ors* (2019) SCC OnLine Del 10036

Section 57 of the Indian Copyright Act (ICA)[31] establishes the right to paternity and integrity, aligning with moral rights specified in the Berne Convention, 1886. For deep fakes, Section 57(1)(b) of the ICA is crucial, addressing distortion, mutilation, or modification of a person's work. Sections 55[32] and 63[33] of the ICA prescribe civil and criminal liability, including damages, injunctive relief, imprisonment, and fines for infringers. While these provisions may effectively deter malicious deepfakes, they may not extend protection to those created for legitimate purposes.

Regarding intermediary liability under Section 79 of the Information Technology Act, 2000 (IT Act)[34], post-Myspace Inc. v. Super Cassettes Industries Ltd. judgement[35], the Delhi High Court harmoniously interpreted the ICA and IT Act. It ruled that in cases of copyright infringement, intermediaries are obligated to remove infringing content upon private party notification, even without a court order. However, challenges persist in detecting deep fakes, posing difficulties for intermediaries in enforcing content moderation policies when addressing such content takedowns.

In a case close to home, Bollywood actor Anil Kapoor filed a lawsuit upon discovering AI-generated deepfake content that utilized his likeness and voice to create GIFs, emojis, ringtones, and even sexually explicit material. In the lawsuit titled Anil Kapoor v. Simply Life India and Ors.,[36] the Delhi High Court protected Mr. Anil Kapoor's persona and personal attributes against misuse, particularly through the use of AI tools to create deep fakes. The court issued an ex-parte injunction, effectively restraining sixteen (16) entities from exploiting the actor's name, likeness, and image, and employing technological tools like AI for financial gain or commercial purposes. Similarly, legendary actor Mr. Amitabh Bachchan, in the case Amitabh Bachchan v. Rajat Negi and Ors.,[37] was granted ad interim in rem injunction against the unauthorized use of his personality rights and personal attributes, including voice, name, image, and likeness for commercial purposes.

Deep fakes under the United States Digital Millennium Copyright Act, 1998 -

The key concern in the US revolves around the expansive scope of the fair use doctrine, offering protection to various types of deep fakes, including those with malicious intent. Section 107 of the Digital Millennium Copyright Act, 1998 (DMCA), outlines the four-factor test for fair use, considering the purpose and character of the use, nature of the copyrighted work, amount taken, and effect on potential markets. This doctrine, often embracing "transformative use" as seen in Campbell v. Acuff Rose[38], protects deep fakes by altering the purpose and nature of the original work, creating content with new expression, meaning, or message. Even in cases of substantial copying, if the deep fake is deemed transformative, it may still receive protection under fair use, as established by US courts.[39]

The broad acceptance of transformative use potentially allows the fair use doctrine to cover a majority of deep fake content, regardless of the creator's intention, whether genuine or malicious. This inclusion may protect deepfakes with malicious intent as parodies under fair use, rendering safeguards like notice and takedown and intermediary liability under Section 512 of the DMCA[40] and Section 230 of the Communication Decency Act[41] unavailable.

[31] ICA 1957, s 57

[32] ICA 1957, s 55

[33] ICA 1957, s 63

[34] The Information Technology Act 2000 No.21 Acts of Parliament 2000 (India)

[35] *Myspace Inc v Super Cassettes Industries Ltd* (2016) SCC OnLine Del 6382

[36] CS(COMM) 652/2023 and I.A. 18237/2023-18243/2023

[37] 2022 SCC OnLine Del 4110

[38] *Campbell v Acuff Rose*, 510 US 569 (1994)

[39] *Patrick Cariou v Richard Prince*, 714 F.3d 694 (2013); *Rogers v Koons*, 960 F.2d 301 (1992); *Leibovitz v Paramount Pictures*, 137 F.3d 109 (1998); *Seltzer v Green Day*, 725 F.3d 1170 (2013); *Blanch v Koons*, 467 F.3d 244 (2006); *Bill Graham Archives v Dorling Kindersley Ltd*, 448 F.3d 605 (2006)

[40] 17 U.S.C. §512

[41] Communication Decency Act 47 U.S.C. § 230 (1996) (USA)

In the US jurisdiction, the absence of legal protection, including the right to the author's reputation and attribution, poses an additional challenge. While Article 6 bis of the Berne Convention, 1886 addresses these rights globally, the protection in the US is limited to authors of visual arts under the Visual Artists Rights Act of 1990[42], excluding authors of other copyrighted works. This creates a precarious scenario where authors may struggle to safeguard their work and reputation when affected by deepfake technology.[43]

Deep fakes under the United Kingdom's Copyright, Designs, and Patents Act 1988 -

UK law safeguards fair dealing through Section 29[44] and Section 30 of the Copyright, Designs and Patents Act 1988 (CDPA). These sections establish specific exceptions within the CDPA framework, allowing the use of copyrighted material without the owner's permission in certain situations. The exceptions cover non-commercial research, private study, criticism/review, or reporting current events. While the UK statute doesn't define fair dealing, Lord Denning in Hubbard v. Vosper[45] stated that determining fairness is a matter of degree. Various parameters have since emerged, such as the nature of the work, method of obtaining it, amount appropriated, character/use, commercial nature, motive, impact on the market, and the availability of alternative non-copyrighted work. Fair dealing also extends to works like parody, caricature, or pastiche under Section 30A,[46] Schedule 2 (2A) of the CDPA.

While the UK's concept of fair dealing, akin to India's, has faced criticism for its perceived inflexibility, the outlined stance allows for flexibility in addressing deep fakes. Legitimately created deepfakes may find justification under research or pastiche grounds. The Civil Division of the England and Wales Court of Appeal, in the Hyde Park Residence Ltd v. Yelland & Ors case,[47] emphasized the significance of the alleged infringer's motive when considering fair dealing, particularly applicable to deepfakes with malicious intent.

Other countries such as The European Union have implemented the Digital Services Act, which mandates social media platforms to comply with labeling obligations, thereby promoting transparency and assisting users in verifying the authenticity of media.[48] South Korea has enacted a law that deems the distribution of harmful deep fakes illegal, with offenders facing penalties of up to five years of imprisonment or fines of up to 50 million won (approximately 43,000 USD).[49] Also, in January 2023, China, through the Cyberspace Administration of China, the Ministry of Industry and Information Technology, and the Ministry of Public Security, emphasized the necessity of clear labeling for deep fakes to prevent public confusion.[50]

[42] Visual Artists Rights Act 17 U.S.C. §106A (1990) (USA)

[43] 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)

[44] CDPA, s 29

[45] *Hubbard v Vosper* [1972] 2 QB 84

[46] CDPA, s 30A

[47] *Hyde Park Residence Ltd* (n 45)

[48] Khan, R. (2023, June 26). UK considers clear labeling law to combat AI deepfakes. Open Access Government. https://www.openaccessgovernment.org/uk-considers-clear-labeling-law-combat-ai-deepfakes/161861/

[49]Lawson, A. (2023, April 24). A Look at Global Deepfake Regulation Approaches. RAI Institute. https://www.responsible.ai/post/a-look-at-global-deepfake-regulation-approaches#:~:text=The%20EU%20has%20proposed%20laws

[50] Kang, L. (n.d.). China's first-ever deepfake rules go into effect, a positive move for tech-oriented companies - Global Times. Www.globaltimes.cn. Retrieved January 8, 2024, from https://www.globaltimes.cn/page/202301/1283499.shtml

Conclusion

The intricate and diverse applications of deepfakes necessitate lawmakers and the judiciary to consider the underlying motives when determining whether copyright protection should apply. The exhaustive fair dealing provision in Indian Copyright legislation fails to recognize the potential legitimate uses of deepfakes, such as in entertainment, education, and MedTech, alongside its primary focus on preventing malicious use. While this approach seems effective in addressing the misuse of deepfake technology, it falls short in acknowledging its legitimate applications. In contrast, the more permissive approach of US copyright law provides a potential avenue for both well-intentioned and maliciously created deep fakes to be protected under transformative use. The criteria established by the UK judiciary enable deep fake creators to make a case for fair dealing protection.

On January 9, 2023, the Ministry of Information and Broadcasting issued a cautionary advisory to media organizations, urging them to exercise prudence when broadcasting content susceptible to manipulation or tampering. The Ministry further recommended that media outlets explicitly label any manipulated content as "manipulated" or "modified" to ensure viewers are informed about the alterations.

Although India currently lacks specific laws addressing deep fakes, there exist legal provisions and government initiatives that could potentially be employed to tackle the issue. With the increasing prevalence and sophistication of deepfakes, the Indian government will likely take additional measures to address the problem and safeguard individuals from potential harm.