International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

# Navigating the Legal Framework for Deepfake Technology in the Era of Intellectual Property and Personal Rights

**P Jeevetha**

Student, LLM-IPL, School of Law, CHRIST University, Central Campus, Bengaluru

**ABSTRACT**

Emerging AI-based technologies like deepfake are paradigms that will add challenges to intellectual property rights (IPR), which include copyright, trademark, and moral rights, threatening privacy, integrity, and more. Deepfakes could also violate copyright, including potentially through the fair use doctrine, which allows for the limited use of protected work without permission. Because transformative use often applies, however, placing such content within the existing copyright protection framework is not cut and dry and must be balanced against the right to freedom of expression for users. They confuse the evident misrepresentation of an endorsement or affiliation and mislead consumers through not telling the truth of a particular service/product or issuer of the service/product, which can be challenged on the basis of trademark infringement. Also, the utilization of deepfake technology, like the use of a live man's appearance without his/her consent, constitutes a violation of the man's-person's personal rights and harms his reputation. This tussle, like the current legal schism, does little to account for the rapid proliferation of deepfakes — particularly the unsanctioned or exploitative use of that sort of digital content.

This paper studies the lack of legal protection (namely copyright and personality rights) and the shortcomings of existing intellectual property regulations to combat the dangers posed by deepfakes. It also engages with potential legislative weeding and how to preserve protections from unearned abuse in the digital realm.

**Keywords**: Deepfakes, Intellectual Property Rights (IPR), Copyright Infringement, Personality Rights, Legal Protection.

## 1. INTRODUCTION

Every new technology comes with the potential for abuse, and deepfake technology is no exception. Deepfakes can be used as a medium of spreading misinformation, altering the popularity of a public by manipulating their video, damaging the reputation of a person/entity, identity theft with this, etc. Deepfakes can thus also erode the credibility of visual and auditory evidence - representing serious challenges to media authenticity and trust. Although deepfakes can manipulate visual media, the potential ramifications of their use–by providing a narrative devoid of a visual connection–creates a new narrative that has spread misinformation and acts as a deceiving tool, proved to be fatal to democratic processes in

that this ability can sway the public perception regarding political events or public figures[1]. To help them, researchers are working on various methods of identifying manipulated data, such as deep neural networks (DNN), computer vision algorithms and forensic analysis[2].

The ethical implications of the misuse of copyrighted content for deceptive or public opinion-manipulating purposes can be very serious. Deepfakes can be used to create malicious and damaging materials, such as revenge porn or fake news, that can spur violence, inflict emotional pain and ruin people's reputations. As deepfakes typically involve the unauthorized use of original works, they most commonly come into the realm of copyright law. This practice may infringe on Copyright, as it undermines the exclusivity that creators hold on their original content.[3] The proliferation of deepfake technology also challenges trademark law. Ultimately, deepfake technology can be misused to redirect the consumer perceptions about the use of brand endorsements or affiliations, which can lead to market confusion. Deepfakes also raise important concerns around deepfake implications, in addition to copyright and trademark issues. Deepfakes can be employed to create false or misleading material that portrays individuals in an untrue manner, putting their reputations at risk or perpetrating fraud.

Personality rights safeguard an individual's identity in the digital realm.[4] But deepfakes threaten these rights by enabling unauthorized use of one's likeness.[5] Trademark law also faces challenges as deepfakes can misleadingly imply endorsements or affiliations.[6] Copyright issues arise when deepfakes manipulate protected content without permission.[7] As technology rapidly evolves, legal frameworks must adapt to address these emerging concerns.[8]

The increased use and development of such techniques adds weight to the question of how to balance technology with individual rights, and this further reinforces the need to explore how our current legislation is failing to protect individuals from the risks of deepfakes, as well as potential solutions to provide protective measures against the risks presented[9]. To this end, this paper seeks to critically engage these apprehensions, specifically with a lens of deepfakes and the salience of IPR, and proffer routes for legal lexicon that ought to embrace deeper protections for both creators, and out its people, in the new AI epoch.

[1] Riski Septiawan, 'Critical Analysis of AI-Produced Media: A Study of the Implications of Deepfake Technology' (2024) 5(7) Devotion : Journal of Research and Community Service 735, XXXX <http://dx.doi.org/10.59188/devotion.v5i7.747> accessed 26 January 2025

[2] Samer Hussain AL-KHAZRAJI and others, 'Impact of Deepfake Technology on Social Media: Detection, Misinformation and Societal Implications' (2023) 23 The Eurasia Proceedings of Science Technology Engineering and Mathematics 429, XXXX <http://dx.doi.org/10.55549/epstem.1371792> accessed 26 January 2025

[3] 'Deepfakes and Intellectual Property: What You Should Know' (*Romano Law*) <www.romanolaw.com/deepfakes-and-intellectual-property-what-you-should-know/> accessed 26 January 2025.

[4] Radhakrishnan, B., 'Personality Rights in the Digital Age: Challenges and Opportunities' (2022) 14 Journal of Intellectual Property Law & Practice 231.

[5] Robert Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' [2018] SSRN Electronic Journal XXXX <http://dx.doi.org/10.2139/ssrn.3213954> accessed 26 January 2025.

[6] Farish, M., 'Deepfakes and Trademark Law: Navigating a Legal Quagmire' (2021) 35 Harvard Journal of Law & Technology 245.

[7] Tushnet, R., 'Copyrightability of Deepfakes' (2020) 23 Vanderbilt Journal of Entertainment and Technology Law 51.

[8] Caldera, E., 'Reject the Evidence of Your Eyes and Ears: Deepfakes and the Law of Virtual Replicants' (2019) 50 Seton Hall Law Review 177.

[9] 'ScoreDetect Blog | Intellectual Property & Copyright Protection' (*ScoreDetect Blog | Intellectual Property & Copyright Protection*) <www.scoredetect.com/blog/posts/preserving-copyright-in-the-era-of-deepfakes-legal-strategies> accessed 26 January 2025

### 1.1 DEFINITION AND NATURE OF DEEPFAKES TECHNOLOGY

Deepfake technology is the application of AI techniques, most commonly ML algorithms, to create or manipulate images, video, and audio for the purpose of falsifying the original or source material in a convincing manner. Deepfakes involve advanced technologies such as "Deep Neural Networks" (DNN) and "Generative Adversarial Networks" (GANs). This gave rise to convincing synthetic media also composed of such deepfake videos viral on social media these past years. Notably, the low technical expertise and tools needed to construct deepfakes can allow such content to be readily created by anyone and spread online[10]. Because deepfakes can produce convincing forgeries that are nearly indistinguishable from real recordings, they have drawn attention. This method uses a two-step process: firstly, it trains a DNN on a large dataset of real media to identify patterns, and then it uses that information to replace or modify media parts to create new material.

With tools like Deep FaceLab, FaceSwap, and commercial services becoming more accessible to non-experts, deep fakes are becoming more prevalent. Pre-trained models and user-friendly interfaces have lowered the technical barriers, but this has also resulted in widespread misuse. A common misuse of deep fake technology is creating explicit content without consent, which can violate privacy and harm reputations. By fabricating realistic voices and appearances of individuals, deep fakes can be used to perpetrate sophisticated identity theft, leading to severe personal and financial consequences. Furthermore, deep fakes are used for spreading political misinformation, fabricating speeches and actions by public figures, and manipulating public perception.

"When it comes to audio manipulation, deepfake algorithms can accurately mimic voices by analyzing speech patterns, intonation, and tone from a source recording." This makes it possible to create entirely original audio clips with the voice of a specific person. Deepfake algorithms are capable of seamlessly swapping faces or superimposing one person's face onto another in video and picture manipulation, creating the impression that the target person is speaking or doing something they never did.

## 2. DEEPFAKES AND INTELLECTUAL PROPERTY RIGHTS IN DIGITAL AGE

### 2.1. COMPLEX INTERSECTION OF DEEPFAKES AND COPYRIGHT REGIME

The Copyright Act, 1957 is an all-encompassing legislation in India with regard to the protection of original works. Copyright exists only with respect to original works in the literary, dramatic, musical and artistic works (which also includes cinematograph films and sound recording)[11]. How does the Act protect these works from unauthorized usage? It creates ownership-applicable rights; copyright is a bundle of rights, the rights to reproduce, communicate to the public, adapt and translate the work[12]. Deepfakes significantly utilize existing copyrighted materials without authorization through manipulation or integration of original content into new works. This often occurs when AI algorithms are trained on large datasets that include copyrighted audio, video, or images without consent from the original rights holders. For example, an individual creating a deepfake may extract scenes from a movie to superimpose the face of a celebrity onto another character, effectively creating a new video that violates the copyright of the original film.[13]

[10] Stamatis Karnouskos, 'Artificial Intelligence in Digital Media: The Era of Deepfakes' (2020) 1(3) IEEE Transactions on Technology and Society 138, XXXX <http://dx.doi.org/10.1109/tts.2020.3001312> accessed 26 January 2025.
[11] "Section 13 of the Copyright Act, 1957"
[12] "Section 14 of the Copyright Act, 1957"
[13] 'Unmasking Deepfakes: Navigating the Copyright Quagmire' (*Cardozo AELJ*) <https://cardozoaelj.com/2024/04/05/unmasking-deepfakes-navigating-the-copyright-quagmire/> accessed 26 January 2025.

Section 51 of the Copyright Act explicitly prohibits the unauthorized use of works that fall under the protection of the act. This section states that any person who does any act in relation to the work for which copyright is subsisting without the permission of the owner infringes that copyright. As such, if a deepfake utilizes copyrighted content, it may violate this provision, subjecting the infringer to legal consequences.[14]
Section 57 of the Indian Copyright Act, 1957 grants certain rights to authors and performers. The moral rights of the author: those rights to claim authorship of a work (commonly referred to as the 'right to attribution' or 'right of paternity') and to avoid the distortion, alteration or mutilation of a work to the detriment of an author's reputation (also referred to as the 'right of integrity')[15]. The Delhi High court in Amarnath Senhgal case[16] the Delhi High court ruled that a privileged relation derives from creative authors with their writings and in enforcing this control over an author's paternity right and integrity right is imperative. These do not constitute rights that can be disavowed or nullified in a contract in an assignment. As there is a prospect of using the protected works by Deepfake without prior authorial permission, it can be classified as distortion, mutilation or modification of a person`s work which creates infringement of right to integrity under Section 57(1) (b) of Indian Copyright Act, 1957.
Intermediary liability is intimately related to copyright law. The sort of content, like deepfakes, that has escaped the bounds of the law most typically travels on social networks or other intermediaries. As per Section 79 of the Information Technology Act, 2000, intermediaries are liable only when they have actual knowledge or on an order from a court to remove illegal content. In Myspace Inc. v Super Cassettes Industries Ltd[17], the Court also held that "intermediaries are obliged to remove infringing content in the event of copyright infringement upon receiving a notice from the concerned private parties, without needing a Court order. Additionally, the draft of the Information Technology [Intermediary Guidelines (Amendment) Rules], 2018 - which is currently under review - mandates that intermediaries proactively monitor and remove illegal content using automated tools like algorithms within 24 hours of receiving an order or notification. Thus, moderating deepfake content online would present a significant challenge for intermediaries in cases of copyright infringement."

**A) Application of Fair use clause**

Fair use is a doctrine in copyright law that permits limited use of copyrighted material without having to seek permission from the copyright holder. In addition, the use of copyright material must be transformative in nature — the second step in determining if a work is a fair use under the copyright Act. In transformative use, the new work must contribute something new or different from the original work. Some of the 4 transformative use elements courts consider include "the purpose and character of the use, the nature of the copyrighted work, the amount and substantiality of the portion used, and finally, the effect of the use on the market for the original work." The US Supreme Court ruled on whether a commercial parody could qualify as fair use, the court recognized that the transformative nature of a work is determined by its ability to create new expression, meaning, or message while also serving a different purpose from the original work[18].
In the Indian context, Section 52 of the Indian Copyright Act, 1957 mentions the principle of fair dealing, but does not define it. "The section contains an exhaustive list of what works do not infringe, essentially

[14] 'What is Deepfake : Is deepfake legal in India?' (*Khurana & Khurana Advocates and IP Attorneys | Home*) <www.khuranaandkhurana.com/2024/04/19/the-use-of-deep-fake/> accessed 26 January 2025.
[15] Section 57 of the Copyright Act, 1957
[16] "*Amarnath Sehgal v. Union of India* 2005 (30) PTC 253 (Del)"
[17] *Myspace Inc. v. Super Cassettes Industries Ltd.* (2017) 236 DLT 478 (DB)
[18] "***Campbell v. Acuff-Rose Music, Inc.***, 510 U.S. 569 (1994)"

making a distinction between bona-fide and malafide users of protected works." Use of a work for private or personal use, such as for personal research; or for criticism or review; or for reporting of current events and affairs, shall not constitute an infringement of copyright as per section 52(1)(a) of the copyright Act It has the approval of Article 13 of the Trade Related Aspects of Intellectual Property Rights (TRIPS) which says that "Members shall confine limitations or exceptions to exclusive rights to certain special cases which do not conflict with a normal exploitation of the work and do not unreasonably prejudice the legitimate interests of the right holder".[19]

It is often criticized that the concept of fair dealing under Indian law is rigid compared to the broad doctrine of fair use in the United States. The distinction between transformative use and infringement can be ambiguous, especially with the emergence of deepfake technology. Although infringers may argue fair use as a defense, deepfakes are not included in the exhaustive list of exceptions under section 52 of the Copyright Act. Therefore, the use of deep fake technologies amounts to copyright infringement and is prohibited for any purpose. In a case, the Hon'ble High Court of Delhi granted a Permanent Injunction in favor of a plaintiff company. The plaintiff, who had enlisted Amitabh Bachchan and Jaya Bachchan as brand ambassadors for Tanishq Jewelry, advertised various photos to promote their classic diamond jewelry. The defendant company violated Section 17(b) of the Copyright Act, 1957 by replicating the plaintiff's advertisement. The plaintiff company, as the first owner of the copyright in the advertisement, was protected by the endorsement agreements which clearly stated their ownership. This case is relevant to this research as it demonstrates that the High Court granted a permanent injunction for copyright infringement and acknowledged the celebrities' rights to publicity.[20]

**B) Deficiencies in the Copyright Act in dealing with deepfakes:**

The current copyright law offers protection against unauthorized use of original works. However, the emergence of deepfakes poses significant challenges that go beyond traditional copyright protections. Deepfakes manipulate or mimic existing images, videos, or audio by blending them with synthetic content created using artificial intelligence (AI). Determining whether the altered content constitutes an infringing derivative work or is entirely new can be difficult. One major limitation of the Copyright Act is its failure to protect personality rights or an individual's right to control their likeness, voice, or identity. Deepfakes often involve the unauthorized use of a person's image or voice, leading to reputational harm and privacy violations. However, copyright law only protects works that are "fixed in a tangible medium," meaning it does not cover a person's likeness unless that likeness is captured in a copyrighted work, such as a photograph or film. While Section 38 of the Act provides some protection for performers' rights, it is limited to live performances or fixed audiovisual recordings and does not extend to a person's likeness being misused in deepfakes. This leaves a significant gap, as celebrities, public figures, and even ordinary individuals have little recourse when their likeness is manipulated using deepfake technology. Indian copyright law is inadequate in offering recourse to individuals who have been exploited through unauthorized digital manipulation[21].

## 2.2. TRADEMARK INFRINGEMENT RESULTING FROM DEEPFAKE CREATIONS

Trademark as defined under Section 2(1) (zb) of Trade Marks Act, 1999 means "a mark which is capable of being represented graphically and which is capable of distinguishing the goods or services of one

[19] "Article 13 of TRIPS agreement"
[20] "Titan Industries Ltd. v. Ramkumar Jewellers 2012 SCC ONLINE DEL 2382"
[21] **Ritu Jain**, *The Indian Copyright Act and Digital Exploitation* 88-95 (Sage Publications 2020)

person from those of others and may include the shape of goods, their packaging; and combination of colors."

Trademark infringement occurs when a person uses a trademark identical or deceptively similar to another party's registered trademark. When a deepfake technology utilizes a trademarked logo, image, or likeness without permission of the proprietor, it can lead to consumer confusion, thereby constituting trademark infringement[22]. Such misuse can dilute the brand's identity and mislead consumers about the source of the content.[23] It could be a unique symbol, logo, word, phrase, design or combining these elements to represent the goods and services offered by the company. This unauthorized use can confuse consumers and take advantage of the reputation of the registered trademark.[24]

Secondly, the creation and dissemination of deepfakes can infringe trademark rights by building upon and/or implying the use of certain trademarks or endorsements that are not accurate. Unauthorised use of a trademark can lead to various legal disagreements, which have led trademark owners to pursue legal action against false representations of their goods and services. Courts may consider and determine if such use of the deepfake would likely create confusion in the minds of the consuming public as to the affiliation, connection, or association of the goods or services in question with the individual whose likeness is being used (whether such individual speaking, singing, or acting, etc.) or as to the origin of the goods or services promoted by the deepfake[25]. Alan Clark vs. Associated Newspapers[26] serves as a prominent example of passing off in the context of deepfakes and impersonation. In this instance, Clark successfully sued the Evening Standard for publishing a spoof diary using his photograph without permission, which misrepresented his identity and brand. Clark's legal victory was based on the misuse of his likeness for commercial purposes, demonstrating how passing off laws protect individuals against misleading representations. The ruling established that unauthorized use of a person's likeness could constitute passing off if it creates confusion among the public regarding the individual's endorsement or association with the material. This case illustrates how legal mechanisms like passing off can address the misuse of deepfake technology, particularly when it comes to public personas.

## 3. PERSONALITY RIGHTS AND PRIVACY CONCERNS RELATED TO DEEPFAKES

### 3.1 What is Personality rights?

In the context of property or privacy rights, personality rights refer to an individual's ability to protect their identity. Celebrities value these rights because their names, likenesses, or voices could be used improperly in advertisements by companies seeking to increase sales. As a result, celebrities and famous individuals should register their names to protect their personal rights. Personality rights cover non-tangible aspects such as mannerisms, acting style, singing style, and overall personality. There are two types of personality rights: the first is the right of publicity, which prevents someone's image or appearance from being used for profit without the owner's permission or payment. Although not identical, this right is similar to using a trademark. The second is the right to privacy, which prevents people's identities from being revealed to the public without their permission.

[22] Section 29 of the Trademarks act 1999

[23] 'Deepfakes and the Legal Avenues to Combat Them' (*Harris Sliwoski LLP*) <https://harris-sliwoski.com/blog/deepfakes-and-the-legal-avenues-to-combat-them/> accessed 26 January 2025.

[24] https://www.indiafilings.com/learn/trademark-infringement-in-india/

[25] Trishana Ramluckan, 'Deepfakes: The Legal Implications' (2024) 19(1) International Conference on Cyber Warfare and Security 282, XXXX <http://dx.doi.org/10.34190/iccws.19.1.2099> accessed 26 January 2025.

[26] Alan Clark vs. Associated Newspapers [1998] 1 W.L.R. 1558

Under this definition, they have a fundamental right under Article 19 of the Indian Constitution's "Freedom of the Press" to procure any and all material to do with celebrities that could even vaguely be framed under "public interest" or "public concern." Celebrities and public figures object to this because it violates their private life and their right to privacy.[27] Each person has the right to defend his life and how it is perceived by the international community. No one, without that person's permission, should have the authority to manipulate how his or her identity is used for profit."

"There is no direct mention of the personality rights as such in the Constitution, but the case of Judge K.S. Puttaswamy v. Union of India[28], recognized the right to privacy as a fundamental right under Article 21 of the Constitution." Privacy is a "right to be left alone that derives from liberty, and anyone who uses another person's identity without the other person's consent is considered to have violated both that person's personality rights and fundamental right to privacy."

**3.2 Potential impact of Deepfakes on Personality and Privacy rights of an individual.**

Deepfake technology poses a serious threat to both individual privacy and personality rights by allowing the unauthorized and deceptive use of personal images and biometric data. This can lead to the creation of inappropriate or defamatory content, causing significant emotional and reputational harm. Potential for impersonation and fraud: The more advanced version of the technology can be used to create content pretending to be someone else leading to privacy issues since people may be misled or manipulated into believing fraudulent content. Even the DPDP Act, 2023, which regulates personal data processing in India and mandates consent, does not address deepfakes specifically. Falling trust on digital media and challenges in tracing and holding accountable actors misusing deepfakes demonstrate this need for existing legal frameworks — or additional legal frameworks — to provide adequate protection in the digital age. Academics have stressed the limitations of existing privacy legislation when it comes to digital manipulation technologies, emphasizing the urgent need for focused legislative response to these nascent dangers[29].

In Indian law, personal attributes such as voice, face, and others fall under personality rights, and are not distinctly recognized. Rather, they fall under copyright and trademark laws. This view goes in line with Anil Kapoor Vs. Simply Life India & others [30] where the use (and also abuse) of Anil Kapoor's persona (image) was before the court, creating deep fake videos and merchandise without his consent. The court ruled that "the unauthorized use of his image was an infringement of his personality and publicity rights, because celebrities' livelihoods often rely on endorsements and public perception. Judge Pratibha M. Singh's ruling emphasized that celebrities deserve legal protection against such conduct, which can violate their rights." Kerala witnessed its first reported deepfake fraud case involving a 73-year-old victim, Radhakrishnan, who fell prey to a scam that utilized deepfake technology. The fraudster impersonated Radhakrishnan's former colleague using an AI-generated voice, asking for urgent monetary assistance. After transferring a sum of ₹40,000, the victim realized he had been scammed and filed a police complaint. Investigations revealed the sophisticated use of AI technology to mimic voices convincingly, leading to a

[27]"https://vajiramias.com/article/how-do-personality-rights-protect celebrities/6389a4049b457a05c56e9aab/#:~:text=In%20India%2C%20the%20publicity%20rights,the%20position%20of%20constitutional%20rig"

[28] *Judge K.S. Puttaswamy v. Union of India AIR 2017 SC 4161*

[29] David A. McGowan, *Deepfakes and the Need for a New Privacy Paradigm*, 59 Hastings L.J. 491, 497 (2022)

[30] "*Anil Kapoor vs Simply Life India & Ors on 20 September, 2023*"

warning issued by the Kerala police about the potential for deepfake scams.[31]

### 3.3 How various courts have dealt with deepfakes and personality rights:

While examining the case filed by the iconic Indian Film actor Mr. Rajinikanth the Madras High Court[32] in "Shivaji Rao Gaikwad vs. Varsha Productions," Inter alia observed that no Statute in India defines "Personality Right". Recently, the Delhi High Court passed an omnibus order or an ex parte ad interim injunction in "Amitabh Bachchan v. Rajat Nagi & ors."[33], banning the public from using the name, image, likeness, voice, or other personal characteristics of one of the most famous actors, Amitabh Bachchan, without his consent. The actor filed a lawsuit against Rajat Nagi & Ors. and the public in the Amitabh Bachchan case (Supra) alleging that they had stolen his name, voice, appearance, and personality traits. The actor claimed in his petition that he had been subjected to misappropriation of his name, image, and voice, mainly by companies that publish books, T-shirt dealers, book publishers, mobile application developers, and people who ran lotteries by unethically partnering with KBC. The decision also opens the door for the nation's legislation protecting personality rights to advance.

## 4. INTERNATIONAL RESPONSES TO REGULATE DEEPFAKE TECHNOLOGY

### 4.1 Federal legislations to combat deepfakes in the United States of America:

As of right now, deepfakes are neither prohibited nor subject to federal regulations in the United States due to a lack of comprehensive legislation. The director of the National Science Foundation is required to finance research for the establishment and assessment of standards necessary for producing GAN outputs and any analogous methodologies established subsequently, in accordance with the Identifying Outputs of Generative Adversarial Networks Act.

Congress is also considering broader legislation to regulate the production, disclosure and distribution of deepfakes; the provisions become a crime if they cause harm. This legislation includes the DEFIANCE Act of 2024 — a bill to provide enhanced rights to relief for individuals harmed by non-consensual uses of manipulated intimate images and for other purposes; The DEEPFAKES Accountability Act aims to amend Title 18 of the United States Code to safeguard national security from threats associated with deepfake technology. Additionally, the Deepfake Report Act of 2019 mandates the Science and Technology Directorate within the U.S. Department of Homeland Security to periodically report on the status of digital content forgery technology. Furthermore, the Protecting Consumers from Deceptive AI Act requires the National Institute of Standards and Technology to form taskforces to develop and recommend technical standards and guidelines for identifying content generated by Generative AI, ensuring that audio or visual material produced or significantly altered by Generative AI includes a disclosure of its origin.

The UK has developed mechanisms for protecting personality rights, particularly through the Online Safety Act (2023), which targets the unauthorized sharing of explicit deepfakes. This law provides individuals a legal route to seek redress for harmed reputations or privacy breaches due to deepfake manipulations. However, a more comprehensive framework addressing all forms of personality exploitation through deepfakes remains in discussion, revealing a commitment to enhancing protections

[31] Indian Cyber Squad, 'Case Study: Kerala's First Deepfake Fraud' (*Indian Cyber Squad*, 27 November 2023) <www.indiancybersquad.org/post/case-study-kerala-s-first-deepfake-fraud> accessed 26 January 2025.
[32] *Shivaji Rao Gaikwad v. Varsha Productions (2015) 62 PTC 351*,
[33] *Ajinomoto Co Inc vs Dattatrey Studios & Anr CS (COMM) 822 OF 2022*

for individuals while balancing the freedom of expression[34]. A landmark Judgment for Personality Rights decided by California Court where Young & Rubicam, Ford Motor Co.'s (Ford) (Defendant) ad agency unable to get Bette Midler (Plaintiff) to re-create her 1970s hit Do You Want to Dance for its television commercial promoting Ford (Defendant), so it hired a former Plaintiff backup singer to impersonate her voice. This case established a treatable tort under the Copyright Act if a celebrity's trademark voice was used by a seller to sell a product generating fraudulently that something was theirs even if it was not. This case had set a benchmark as it has been cited in various courts of various countries to claim the celebrity's personality rights. This case is of great relevance to the present study as it is a landmark judgment in the US for personality rights restraining anyone from impersonating and using a celebrity face, voice etc., for commercial purposes[35].

**4.2 European Union's new rules for combating deepfakes:**

Deepfake technology has been named by University College London (UCL) as one of the biggest hazards facing modern society. The border between fact and fiction is blurred by deepfakes' lifelike portrayals of people and locations, raising issues with privacy, ethics, and security, as well as undermining public confidence in the government, media, and public figures. They provide difficulties for social media platforms and news organizations, among others, when it comes to content moderation. The main issue is that these systems have the ability to produce incredibly lifelike deepfakes or fake news, and they can even be employed to support extensive misinformation campaigns. The EU AI Act would put new regulations on deepfakes, even though the EU has already demonstrated its intention to regulate them within current legal frameworks.

The AI Act defines a deepfake as an 'AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful'. The AI Act recognizes that deepfakes alter reality by passing off incorrect information as fact, in addition to creating false impressions. Truthfulness requirements coupled to authenticity could result in a stricter legal standard. Deepfakes are not totally prohibited by the AI Act. However, it attempts to address the problems caused by deepfakes by placing stringent criteria on openness for both AI system providers and consumers.

The AI Act determines that it is acceptable to compel system providers to embed technical solutions given the expanding capabilities and general availability of AI systems, the quickening pace of technological advancements, and the necessity for novel approaches and methodologies to track the origin of information. These solutions would allow for the detection and tagging of output generated or manipulated by an AI system rather than a human in a machine-readable manner. The AI Act exempts from this labelling requirement, in order to maintain proportionality, AI systems that primarily serve as assistants for normal editing or AI systems that do not materially change the input data supplied by the deployer or its semantics.

The AI Office, which is being established in accordance with the AI Act, is tasked with encouraging and facilitating the development of codes of practice to make it easier to carry out the duties associated with identifying and classifying artificially generated or altered content. The European Commission may either issue an implementing act outlining uniform guidelines for carrying out those duties, or it may adopt

[34] 'Deepfakes And Intellectual Property: Understanding Legal Challenges And Protections In The Artificial Intelligence Era' (*Mondaq - Law Articles and Insights*) <www.mondaq.com/india/new-technology/1464126/deepfakes-and-intellectual-property-understanding-legal-challenges-and-protections-in-the-artificial-intelligence-era> accessed 26 January 2025.

[35] "Bette Midler v. Ford Motor Company [849 F.2d 460 (1988)],"

implementing acts to ratify those codes of practice. The openness requirements of the AI Act might or might not be sufficient to reduce the dangers of deepfakes and support an informed public. This will also depend on whether other EU businesses implement robust deepfake detection or if they simply search for watermarks and assume that the problem has been solved.

### 4.3 Legal framework relating to regulation of the deepfakes in India

**Deepfakes are not regulated directly, but indirectly through various provisions such as the following:**

1. The **IT Act, 2000** is India's primary legislation dealing with cybercrime and electronic commerce. While the IT Act does not directly address deepfakes, certain provisions under this act are relevant:

- Section 66E: This section penalizes the capturing, publishing, or transmitting of private images without consent, which can be applied to deepfake content that violates privacy by digitally manipulating someone's image or video. The offence is punishable by a maximum of three years of imprisonment, or with a fine of ₹2 lakh. Likewise, the Section 66D of IT Act punishes persons who use computer resources or communication device by means of carrying on fraud or impersonation. The penalty for this offence is imprisonment for a term which may extend to three years and/or fine of ₹1 lakh.
- Section 67: This section criminalizes the publication or transmission of obscene material in electronic form. This section would likely cover deepfakes, especially when used to create pornographic or otherwise objectionable content.

2. Defamation is governed under Indian Penal Code (IPC) under Sections 499 and 500 for when the image of a person is tarnished due to a misrepresentation or false statements. Deepfakes, particularly when they are used to damage someone's reputation, could be addressed through these provisions. Section 499:Definition of defamation and would be relevant to deepfakes where it defames someone and damages their reputation; and Section 500: Punishment for defamation, even if it is an evil fabricated through a deepfake.

### 4.4 Comparative Analysis on Deepfake technology

Globally, there is growing concern about the need for comprehensive theory legislation for deepfakes. International organizations, including the World Economic Forum and its member countries, the United Nations and member countries, are starting to collectively grapple with how to appropriately regulate this technology to ensure that victims retain their legal protections. Such discussions undermine the importance of balancing protection of free expression and, indeed innovation, with preventing harmful damage, he added. A few states in the US have already started regulating deepfakes. California and Texas have laws that target deepfakes of adult content and for political misinformation, among other things. Congress is still working out how to tackle deepfakes federally, including whether to create new laws or rely on existing statutes. EU's Artificial Intelligence Act divides Ai systems according to risk class High-risk AI systems, such as some kinds of deepfakes, will need to come with stronger transparency, accountability and human oversight requirements.

Deepfakes are technology that has been widely discussed and become very concerning by their unique ability to disseminate disinformation, commit fraud and assassinate individuals' character. Deepfakes aren't always illegal, but can violate intellectual property rights, privacy laws, and laws prohibiting defamation, harassment and fraud. The courts remain somewhat haphazard and inconsistent, in large part because the emergence of deepfake technology preceded regulations like the ones we have now. Bridging this divide will demand qualitatively different approaches to defining acceptable versus harmful use,

clearer legal boundaries, and even enforcement that is equitable and fair. Such regulation is being pursued by groups like the United Nations and the World Economic Forum — finding the middle ground between bullying harm versus protecting free speech and innovation at scale. In USA, EU, South Korea and Australia, much effort underway is making targeted legal frameworks to fight the nefarious threats of deepfakes while enabling fair use of the technology.

## 5. THE NEED FOR COMPREHENSIVE LEGAL REFORMS

It may be a heavy job, but the goal of tackling the global challenges that deepfakes have to offer is vital. Existing laws on defamation, harassment, privacy and intellectual property need to be updated so that deepfakes and their potential consequences are comprehensively addressed in India. Tighter legislation would help mitigate the risks associated with deepfakes, Rowling added. India's IP laws need a major update, which should include a clearer definition of the extent to which AI-generated content is protected under IP law. Current copyright law requires human authorship and creativity in order to be protected. Even considering that India will be the first country to ensure AI co-author, AI is not a legal person yet and can only be protected as a person (natural or artificial) under the Copyright Act 1957. The IP regime has to be appropriately amended in light of the current issues. In response, the Ministry of Commerce and Industry stated in the Rajya Sabha that AI-generated work falls under the purview of current copyright regulations, although this position ignores important nuances. Legislation may concentrate on making it illegal to create and disseminate AI Deepfake with the intention of misleading or hurting people.

Without permission, using a celebrity's deepfake can violate their rights to publicity, hurting their reputation and leaving them up to exploitation. New challenges posed by deepfakes are not well addressed by current copyright legislation. In order to prevent manipulation, authors need to actively look for infringements on the internet. Takedown procedures are erratic, sluggish, and frequently fail to halt the spread of viral content. The strongest line of defence against the threat of deepfakes is a combination of technology, appropriate practices, legal protections, and increased public awareness.

## 6. Suggestions for Legal Reforms in India

### 1. Strengthening Copyright Laws

This would require an amendment in the Copyright Act, 1957 — Since deepfake technology can be used to easily manipulate or use copyrighted material without authorization, an amendment in the Copyright Act, 1957 is a sound move. In short, it's time for a better definition of transformative use, especially when most AI-generated content could plausibly be called transformative, at least in the digital age.

### 2. Extension of Personality Rights

Indian laws must also provide specific rights to an individual to safeguard his likeness, image, voice or other personal identifiers from being manipulated or exploited without his authorization through these deepfake technologies. Criminal remedies would not be enough to prevent misuse of identities through deepfakes, as they only respond to conduct that is detrimental to public order, making amendments for civil remedies a necessity, particularly those that offer civil remedies for the misappropriation of identity that harms a person's reputation or privacy through the Indian Contract Act or tort law, amongst others.

### 3. Reinforcement of Trademark Protections

Deepfakes often lead to the misleading uses of a brand's trademarks, image, or false endorsements. Amendments in the Trademarks Act, 1999 with specific provisions prohibiting misuse of trademarks in deepfake content and stringent penalties for misleading consumers about brands should be made. Against

Uses of Trademarks in Deepfakes Online: Online marketplaces must have a duty to monitor and remove unauthorized use of trademarks in deepfakes, to prevent confusion in the marketplace and protect the integrity of brands.

**4. Data Protection and Privacy Law**

Deepfake technology poses distinct challenges when it comes to data protection and privacy. In light of such challenges, the Digital Personal Data Protection Act, 2023 establishes a strong framework, focusing on consent, data security, and individual rights. Despite some progress, the emerging nature of deepfake technology renders legal and technological efforts as something that must constantly be updated.

## CONCLUSION

The copyright issues at play here are complicated further by the fact that copyright law around the world varies significantly. While technology evolves at a breakneck pace, the legal system continues to lag behind solving these new issues. Its effects are felt in India which calls for urgent response. A unique law for personality rights — such as that in Guernsey — could provide invaluable protection. India has an opportunity to step up and identify and act on this challenge holistically. But to be honest, regulating deepfakes won't fix the root cause of the issue. Although existing laws protect against malicious deepfakes and enable victims to seek legal recourse, enforcement is tricky. Likewise, addressing these concerns and potential criticisms — for example, the absence of sanctions for failing to comply with transparency obligations — will be critical for moving forward. We need to think critically about how new regulations such as, for example, the AI Act, could address these issues in a meaningful way. India must proactively address deepfakes' challenges to intellectual property and personal rights.[36] Strengthening copyright laws, extending personality rights, and reinforcing trademark protections are crucial steps.[37] The Digital Personal. Data Protection Act, 2023 is a positive development but constant updates are necessary.[38] While regulating deepfakes alone won't eliminate the root issues, Its vital for India to holistically identify and act on these challenges.[39] As technology rapidly advances, the legal system must keep pace to effectively protect individuals and their rights in the digital age.[40]

[36] Radhakrishnan, B., 'Personality Rights in the Digital Age: Challenges and Opportunities' (2022) 14 Journal of Intellectual Property Law & Practice 231.
[37] Robert Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' [2018] SSRN Electronic Journal XXXX <http://dx.doi.org/10.2139/ssrn.3213954> accessed 26 January 2025.
[38] Farish, M., 'Deepfakes and Trademark Law: Navigating a Legal Quagmire' (2021) 35 Harvard Journal of Law & Technology 245.
[39] Tushnet, R., 'Copyrightability of Deepfakes' (2020) 23 Vanderbilt Journal of Entertainment and Technology Law 51.
[40] Caldera, E., 'Reject the Evidence of Your Eyes and Ears: Deepfakes and the Law of Virtual Replicants' (2019) 50 Seton Hall Law Review 177.