E- Journal of Academic Innovation and Research in Intellectual Property Assets (E-JAIRIPA)

Vol. V (ISSUE I) JAN -JUNE 2024, pg. 1 - 13

NAVIGATING THE FRONTIER: BALANCING PERSONALITY RIGHTS, PRIVACY, AND INTELLECTUAL PROPERTY IN THE AGE OF DEEPFAKE TECHNOLOGY

Aranya Nath[1] *& Gautami Chakravarty*[2]

Abstract

The advent of Artificial Intelligence and Big Data has led to advancements in technology, but it is crucial to understand the challenges and privacy concerns that come with these technologies. In India, legal experts are working to address privacy issues caused by Deep Fake Technology. The authors aim to discuss the regulatory framework to address these issues, focusing on the ethical implications of deepfake technology in media and entertainment. They propose that criminal provisions in copyright legislation, such as 65(A) & (B), do not adequately address the challenges posed by AI. They also propose a holistic view of performers' rights reform, providing legal precedents. The paper also discusses the ethical implications of deepfake technology in media and entertainment and suggests new legislation that integrates innovation with individual rights protection. It also discusses technical improvements in deepfake detection and prevention and how these technologies can be integrated into legal and intellectual property protection measures.

***Keywords*:** Copyright Law, Performer's Rights, Rome Convention, Deepfake Technology, Privacy Rights, Personality Rights.

[1] Ph.D Scholar, Damodaram Sanjivayya National Law University, Sabbavaram Visakhapatnam.
[2] LLM (IPR Specialization) National Law University Judicial Academy Assam.

Introduction

Deepfake technology has posed significant issues and potential in a variety of fields, notably in the realms of personality rights, privacy, and intellectual property (IP). Deepfakes, which use powerful artificial intelligence to produce very realistic but manipulated audio and visual content, have swiftly progressed, becoming more accessible and complex. This technological breakthrough raises serious concerns about how the boundaries of individual rights and intellectual property are being challenged and potentially violated. Therefore, It is challenging to identify the true and morphed image as the public generally believes what they see in their own eyes. As a result, women became victimized early in online media but nowadays after the broad emergence of Artificial Intelligence & Big Data it became more prevalent as a result Deepfake Technology become much more prevalent in today's reality. Even Legal Scholars & IP policymakers are researching to find legislation that could help the victim & control Deepfake Technology. It is an outcome of Artificial intelligence linked with cloud computing and Big Data.[3]

Personality rights, which include the protection of an individual's name, likeness, and persona, are increasingly under attack as deepfakes make it feasible to construct convincing representations of people without their knowledge. Unauthorized use of one's likeness for commercial or libelous reasons carries considerable concerns, testing current legal structures that were not prepared to deal with such sophisticated types of digital manipulation. As deepfake technology enables the fabrication of incredibly realistic but fraudulent pictures and videos, the potential for abuse, such as fake endorsements, identity theft, and reputational damage, has never been higher. Deepfake technology also has a significant impact on privacy. The capacity to create realistic material can result in serious violations against individual privacy, such as nonconsensual pornography and fabricated accusations[4]. These assaults not only violate human liberty, but they also offer problems to present privacy rules, which may fail to handle the intricacies of deepfake-related privacy breaches. The need for enhanced legal protections that can successfully address these new types of privacy intrusions is urgent. The study is conducted to create a significant inception among the readers to understand the conundrums of deep fake technology that arises in today's tech-based era owing to the advent of AI. Copyright law is driving significant legislation in curbing the deepfake technology as there is an absence of legislation that looks into the personality rights of the performers even though punitive punishments are there in the copyright law and its function will be discussed here. The research paper is formulated with doctrinal and analytical. The researchers will try to

[3] Artificial intelligence and intellectual property: call for views, GOV.UK (2020), https://www.gov.uk/government/consultations/artificial-intelligence-and-intellectual-property-call-for-views (last visited Nov 23, 2023).

[4] Yisroel Mirsky & Wenke Lee, *The Creation and Detection of Deepfakes: A Survey*, 54 ACM COMPUT. SURV. 1 (2022).

analyze the concept of deep fake technology and how copyright law supports the ongoing burning issue. Lastly, data was collected through various journals, periodicals, websites, etc.

Deepfakes technology overview

Artificial intelligence (AI) programs that merge mix, replace, and superimpose photos and video clips to create fake videos that look real are known as deep fakes. In 2014, Ian good fellow made it. Even without the user's consent or permission, they could use deepfake technology to create, for instance, a humorous, pornographic, or controversial film of a person speaking. As users tend to stick with the group, deepfakes target social media platforms where conspiracies, rumors, and false information may spread quickly.[5]

The creation of deep-fake technology

Generative adversarial networks (Gans) are a machine learning approach used to construct deep fakes. A Gans is made up of two neural networks that have been trained on a significant number of actual photos, videos, or audio recordings: a system for discrimination and a generator. The machine learning system, similar to the generated image, develops artificial data that reproduces what is present in the training collection. Following that, the network of discriminators analyses the authenticity of artificial information and provides feedback to the generation on ways it enhances what it produces. The procedure is carried out several times while the generator develops fake content that is extraordinarily genuine. It's challenging to distinguish from actual data. During such duration, the discriminator and generator acquire knowledge about one another. The training information is used to generate deep fakes, which may be used to make video and image deep fakes in several methods:

Face swap: changing the face of one individual for the one in the video;

Attribute editing: changing attributes of the individual in the video, such as hairstyle or color;

Face re-enactment: transferring facial reactions from a single face onto the person in the target video; and

A completely synthetic material: real material is utilized to learn how individuals seem, but the final representation is purely fake.

Deepfakes detection

Deepfake Technology keeps developing and improving, consequently, deepfake detection algorithms must be updated regularly to stay up with the current advances. Currently, the most effective way to tell if a piece of media is a deepfake is to utilize a combination of various detection techniques and to be wary of anything that seems too tempting to be true. The following is some of the most prevalent methods for

[5] Hrisha Yagnik, Akshit Kurani & Prakruti Joshi, *A Brief Study on Deepfakes*, 07 5 (2020).

detecting deepfakes:

1. Graphical artifacts: some deepfakes include evident graphical objects, such as strange facial expressions or blinked eyes taken advantage of to detect forged footage.[6]

2. Misalignment of audio and video: with some deep fakes, the audio and visual content might not correspond precisely, suggesting that the information alters. For instance, an individual's lip motions in deep fake footage might not correspond to the audio exactly, or the audio might include background noise or reflections that don't exist within the video[7] such kinds of audio-visual inconsistencies might indicate whether the subject matter alters.

3. Deep learning recognition: Deep Machine learning techniques, including deep neural networks, can be developed on an enormous collection of real and fake pictures, videos, or audio to detect deep fakes. Artificial information patterns and artifacts such as strange facial movements, inconsistent eye blinking causes, and audio-visual incompatibilities are learned by computer. Once trained, the deep learning system may examine previously unknown media for deepfakes. If the algorithm detects fake content, it can flag it for individual scrutiny or further evaluation.[8]

Deep Fakes, Copyright & Personality Rights

Deepfakes, which are classified into four usage categories, may help tiny start-up businesses with sales and marketing, comedy or parody, revenge porn, and political campaigns. A neighborhood boutique selling customized dresses, for example, may profit from a deep-fake application that enables buyers to try on the outfits, making purchasing decisions easier. Deepfakes may also be humorous or satirical, as evidenced in the viral "TikTok films of Tom Cruise licking a lollipop only to discover chewing gum in the center." Thousands of forged votes emerged in Ohio in 2016,[9] fueling fears among voters that elections had been manipulated. The image and identity of the individual who discovered the phony votes were proven to be a deepfake.

Revenge pornography consists of sexual representation photographs and films made public by an angry former partner, which can have major long-term negative consequences in one's personal and professional life. Women are exposed to deep-fake videos. It has been estimated by the report of UN SDG that more

[6] Shruti Agarwal et al., *Protecting World Leaders Against Deep Fakes*.
[7] Zhou and Lim - 2021 - Joint Audio-Visual Deepfake Detection.pdf, https://openaccess.thecvf.com/content/ICCV2021/papers/Zhou_Joint_Audio-Visual_Deepfake_Detection_ICCV_2021_paper.pdf (last visited Nov 24, 2023).
[8] Agarwal et al., *supra* note 6.
[9] Why the Manoj Tiwari deepfakes should have India deeply worried, https://theprint.in/tech/why-the-manoj-tiwari-deepfakes-should-have-india-deeply-worried/372389/ (last visited Oct 21, 2022).

than 85% of women are subjected to such kinds of deep fake videos owing to gender biases. [10]

In the future, Ethical issues about deep fakes for revenge pornography and politics necessitate a reconsideration of whether deep fakes deserve to be granted stronger intellectual property protection. Deep fakes used to produce meaningful material, marketing & customization of social media posts in local dialects, for example, are inventive and imaginative, necessitating an increased balanced discussion of the subject.

The justification over Deepfakes raises questions about the control of free speech, since an outright ban can indicate controlling the freedom of speech, a practice contradictory to democracy, free expression, and trust. It poses three concerns:

a) Are Deep Fakes legally covered by the copyright regime?

b) How may exceptions and constraints help to balance the deepfake debate?

c) Concerning the wake of deep fakes how the relationships between freedom of speech and IP protection, as specified in the Constitution of India should be balanced?

Protection of Certain Aspects of Personality Rights under IP Laws and Other Laws

"Article 21 of the Indian Constitution comes closest to maintaining personal rights in India. Subsequently, the legislation excludes the economic part of personality rights, Indian courts used to rely on provisions under copyright and trademark law to preserve certain aspects of personality rights." Passing off has been used to safeguard personal rights in various circumstances. While present IP rules may appear acceptable, various features and complexities remain neglected, rendering them ineffective.[11] The courts have overlooked these realities and granted remedies, leaving just a few personality traits protected under the current intellectual property regime. In certain scenarios, courts have read personality rights safety as well-known trademark protection.

In "*D.M. Entertainment v. Baby Gift House*, [12] the case involving the financial implications of personality rights, wherein the court awarded relief by utilizing trademark law issues such as passing off and false endorsement. This case emphasizes the need to have a thorough awareness of the rights and intricacies underlying personality rights in India."

[10] Edvinas Meskys et al., *Regulating Deep Fakes: Legal and Ethical Considerations*, 15 JOURNAL OF INTELLECTUAL PROPERTY LAW & PRACTICE 24 (2020).
[11] Agitha T.G & N.S. Gopalakrishnan, *The Imperial Copyright Act 1911 and the Indian Copyright Law*116 (2013).
[12] Daler.pdf, https://spicyip.com/docs/Daler.pdf (last visited Nov 24, 2023).

Existing Legal Instruments for the Protection of IP Rights

The court authorized an injunction for infringement of a registered mark in a well-known personality under trademark and passing off. This was because the plaintiff's caricature was covered under the preview of the goods offered, resulting in a violation of the registered mark. The exploitation of a well-known personality's unique identification trait also constitutes an act of unfair competition worthy of a passing-off claim. Unauthorized use of their distinctiveness also creates a deceitful impression that the plaintiff has licensed or has some relationship with the defendant's goods or services, akin to fraudulent endorsement.

In exceptional circumstances, the court may use copyright to protect personality rights, even if the Act does not explicitly specify the same. Certain provisions of the Copyright Act might be beneficial remedies against violation of personal rights. "Section 2(qq),[13] for example, defines performer if personality is under the ambit of performer definition; Section 38, where performer right stated, prohibits the unauthorized promotion of one's performance. Section 57 also gives ethical protections in specific instances and prohibits the unauthorized promotion of one's performance. Section 57 also gives ethical protections in specific instances."[14]

In "*Titan Indus. Ltd. v. Ramkumar Jewellers*,[15] the court attempted to address the plaintiff's entitlement to be the first creator of the work while considering the plaintiff's personality as a performer." Along with copyright, the court established elements constituting liability for infringement of the publicity right, with the first being validity, which requires the plaintiff to have an enforceable right in their persona or identity, and the second being identifiability, which requires the celebrity to be recognizable from the defendant's illegal usage. Infringement of the publicity right does not need proof of confusion or untruth if the personality is identified.

Finally, only celebrities have the right to be awarded personality protection based on the traits mentioned above.

Provisions under the Information Technology Act

The Information Technology Act, of 2000 first cyber law in India to regulate cyberspace has provisions dealing with cybercrimes. However, due to the non-comprehensive nature of coverage of cybercrimes under the IT Act, of 2000, the Act alone cannot regulate deepfakes. Some provisions of the IT Act that

[13] copyrightrules1957.pdf, https://copyright.gov.in/documents/copyrightrules1957.pdf (last visited Nov 24, 2023).
[14] Section 57 in The Copyright Act, 1957, https://indiankanoon.org/doc/1710491/ (last visited Jun 14, 2024).
[15] Titan Industries Ltd. vs M/S Ramkumar Jewellelrs on 26 April, 2012, https://indiankanoon.org/doc/181125261/ (last visited Nov 24, 2023).

invoke to deal with deepfakes are explained below. "Under the IT Act, cybercrime is committed if deepfakes are used inappropriately or abused. Section 67 of the Act provides for penalties for the electronic publication or transmission of obscene material and if the deepfake created is inappropriate then it would attract this provision. Section 67A of the Act outlines the penalties for publishing or transmitting material in electronic form that contains a sexually explicit act or conduct and thus a deepfake that contains a sexually explicit act will attract penalties.[16]" Section 67B of the Act criminalizes the publication or transmission of material in electronic form that depicts children engaging in sexually explicit acts or conduct and will apply to deepfakes involving children. The deepfake maker shall be punishable for the offence, under the provided "Section 66C of the IT Act, 2000, if the deepfake content uses any kind of unique identification feature, such as electronic passwords, of a person in a fraudulent manner. It includes a foreign country's identity. In addition, section 66D of the Act penalizes usage of a computer to commit fraud through impersonation." Under "Section 69A, the Central Government has the authority to direct the intermediary to block any such deepfake content if it determines that doing so is necessary for preserving the independence and territorial integrity of India, maintaining India's national security, and fostering cordial relations with other nations." Apart from the computer-related offense, the IT Act punishes for privacy infringement. "Section 66E of the Act outlines the penalties for violating a person's right to privacy as follows: if the accused person intentionally or knowingly photographs, publishes, or transmits an image of a private area of another person without that person's consent, the accused person is subject to a sentence of imprisonment of up to three years or a fine of up to two lakh rupees, or both, depending on the severity of the offense. Another provision in the IT Act that deals exclusively with cyber defamation is Section 66A sending any information via a computer resource that is excessively offensive or has a menacing nature or is to create annoyance, discomfort, danger, obstruction, insult, injury, criminal intimidation, hostility, hatred, or ill will is punishable by this section. However, the Apex Court in "*Shreya Singhal v. Union of India*[17]" nullified this section of the IT Act, making it obsolete. Thus, this provision holds no value in addressing deepfakes. The previous provisions were mainly to deal with deepfake makers. The IT Act also provides for the liabilities of intermediaries. Since intermediaries host deepfake content, Section 79 of the Act regulates their liability. After discovery or court order, the intermediary may remove the content. In *Myspace Inc. v Super Cassettes Industries Ltd,*[18] the Court ruled that intermediaries must remove copyright-infringing information upon private party complaints without a

[16] Cyber Lawyer, *Section 67 of Information Technology Act: Punishment for Publishing or Transmitting Obscene Material in Electronic Form*, INFO. TECHNOLOGY LAW (Sep. 18, 2014), https://www.itlaw.in/section-67-punishment-for-publishing-or-transmitting-obscene-material-in-electronic-form/ (last visited Nov 10, 2022).
[17] Shreya Singhal vs U.O.I on 24 March 2015, https://indiankanoon.org/doc/110813550/ (last visited Nov 4, 2022).
[18] My Space Inc. vs Super Cassettes Industries Ltd. | wilmap, https://wilmap.stanford.edu/entries/my-space-inc-vs-super-cassettes-industries-ltd (last visited Jun 9, 2024).

Court order. Currently, intermediaries are only required to advise users about not posting certain kinds of harmful/unlawful content. Recent IT Rules 2021 establish a legal requirement for intermediaries to make reasonable efforts to prevent users from posting such content. The new clause will ensure that the intermediary's obligation is not a formality.

Copyright Regulations for Deepfake Technology

In the initial stage the most important, concern is whether deep-faked works are protected by copyright law. Deep fakes may be highly creative and entail substantial technological creativity. Could such inventions then be considered copyrighted works? Two criteria must be satisfied to profit from copyright protection. Additionally, there has to be a work, which has to be original in terms of the fact that it is the author's intellectual creation. According to Article 2(1) of the Berne Convention, "literary and artistic works shall include 'every production in the literary, scientific and artistic domain' irrespective of its 'mode or form of expression.[19]" Now it's important to understand the position of the United States & India so that the readers will get a significant inception why it's necessary to make stronger legislation for AI generative content we observe critics that have been expressed in the newspaper about the john-doe order of Anil Kapoor deepfake case. In the US, copyright Legislation deep fakes are regulated by copyright law in the United States. Yet is confusing since Deepfakes may be protected under the theory of fair use, as stated in 17 USC 107.[20] This section considers the purpose and character of usage, such as its commercial nature, the content of the work under copyright, the significance of copying, and its effect on the prospective market value of the copyrighted work. The concept of transformative use established in *Campbell v. Acuff Rose*,[21] permits the law of fair use to be extended to preserve the work when a new meaning or expression is discovered in a work, regardless of whether a significant amount of the work under copyright is reproduced. Deepfakes are also protected under the theory of fair dealing in many cases in the United States since the nature of the work is fundamentally distinct from the copyrighted work and the possibility of inflicting any harm to the potential market of the actual copyrighted work is extremely low. Other laws are utilized to impose responsibilities in situations where deep fake information is slanderous. Moral rights are the rights that preserve the creator's reputation and provide them the right to have their work assigned to them. Based on the legal status of each country, copyright

[19] Berne Convention for the Protection of Literary and Artistic Works, https://www.wipo.int/treaties/en/ip/berne/index.html (last visited Dec 26, 2023).

[20] 17 U.S. Code § 107 - Limitations on exclusive rights: Fair use, LII / LEGAL INFORMATION INSTITUTE, https://www.law.cornell.edu/uscode/text/17/107 (last visited Nov 24, 2023).

[21] Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569 (1994), JUSTIA LAW, https://supreme.justia.com/cases/federal/us/510/569/ (last visited Nov 24, 2023).

law might be utilized as a regulation for deep fakes. Copyright protection extended to cover deep fakes in some areas. As intellectual property intended to encourage innovation and stimulate future innovation, ownership of this specific copyright must be granted to any individual who uses generative adversarial network technologies to generate the deepfake material. For further understanding, the legal personality of artificial importance will analyze possessing rights and discharge responsibilities as the most crucial need for anybody with legal status. Because of the black box issue, one of the biggest challenges arising in the realm of AI is the conundrum within the concept of will. In this instance, it is not possible to conclude that the objective of intellectual property rights for people would be the same as artificial intelligence. As a result, it might be unwise to give copyright to the deepfake technique in and of it. Computer programs are considered literary works in India, decided as required by Article 10 of the TRIPS Agreement.[22] Computer software is deemed a literary work in the US under Section 17 USC 101 and is also considered a literary work under Sec 2(o) in India. Policy concerns and debates must be addressed owing to the advent of deep fake technology within the scope of literary works. In this perspective, granting copyright to the individual who employs the technology to create deep fake material becomes conceivable. If the deep fake material generated isn't included within the ambit of the transforming application results in fair use, it could be considered a derivative work for which permission from the work's initial proprietor is needed.

Deep Fakes & Personality Rights

The interplay of the internet and deep fakes may present an imminent challenge to authorities. Deep fakes entail the artistic modification of videos and pictures. It implies that people are frequently unwilling performers in deep-fake works. Additionally, they might be completely oblivious to the deep-fake work. The work may have already been extensively extended when individuals learn about its existence. In such an instance, the harm to one's personality, and perhaps to the community, may be borderless, irrevocable, and irretrievable. As a result, a discussion of personality rights and privacy is extremely appropriate for building the entire intellectual property rights framework. Personal rights are the least harmonized of the several types of rights. [23]

What intensifies issues is that Deepfakes, in some respects, functions similarly to the pharmaceutical sector. The doctor recommends the medication, the chemist sells it, the patient takes it, and the national

[22] WTO | intellectual property (TRIPS) - agreement text - standards, https://www.wto.org/english/docs_e/legal_e/27-trips_04b_e.htm (last visited Feb 19, 2024).

[23] (PDF) Image Right and Copyright Law in Europe: Divergences and Convergences, https://www.researchgate.net/publication/276039212_Image_Right_and_Copyright_Law_in_Europe_Divergences_and_Convergences#read (last visited Nov 24, 2023).

health authorities pay for it in the pharmacy industry. Three distinct categories of individuals and enterprises are the doctor, the consumer, and the reimbursing authority. Unexpectedly, the Deep Fakes example is somewhat different. A deep fake film's customer is separate from the movie's developer, who has morphed and deep-faked a greater number of images and videos.

Copyright, privacy regulations, and personality rights are all involved in the sharing of original videos, photos, speech, and data in audio-visual material. Consumers, makers, and persons featured in these movies or photographs are frequently separate parties who frequently remain not associated and unknown to one another. This makes it difficult for buyers to feel remorse for the intended receiver of deep-faked work. The link between personality rights and deep fakes is essential to this subject. Individual tastes differ when it involves sharing pictures; some consider it as taking their soul, while others value public examination of their personality. Other parts of personality rights include name, signature, and other distinguishing characteristics.

Now the main concerns that arise over here are the challenging issue of deep fakes & copyright issues for personality rights and why it requires stronger protection though the John Doe Order is there.

Overview of John Doe Order

A John Doe order is a comprehensive injunctive remedy designed to protect the intellectual property rights of the author of artistic works such as films, music, and so on. The expression "John Doe" refers to unknown/ nameless defendants infringers who are accused of some wrongdoing, but their true nature is unknown to the plaintiff. To prevent unnecessary delay and to ensure justice, the court refers to the defendant as "John Doe" until the defendant is recognized. Orders issued by courts in such situations are referred to as "John Doe orders."

Benefits of John Doe order

The John Doe order supports filmmakers/producers and intellectual property owners in their battle against digital piracy and copyright infringement. Producers utilized the John Doe order on numerous occasions to prevent their films from being illegally downloaded from the internet. For the first time, in "UTV *Software Communication Limited v. Home Cable Network Ltd*., the High Court of Delhi issued the John Doe order against the cable television operators that unlawfully transmitted unlicensed copies of films "7 Khoon Maaf" and 'Thank You.'" Following this incident, the John Doe order is now a prevalent instrument within the field of media and appears to be an efficient means to combat piracy.

Deepfakes require stringent legislation- Reasons

As it's known to all, Deepfakes are the generic versions of Artificial Intelligence which has a lot of lacunae in today's tech-based era. Still, now the current IP Laws & IT Laws are trying to curb the issue. Owing to the lack of proper legislation it's become impossible to provide stringent protection.

Furthermore, it exploits certain unscrupulous persons to create fictitious pornographic content and political advertisements, putting the victim's privacy, identity, and protection at threat. Recently, Amitabh Bachchan's Deepfake A/V gives a light to safeguard his publicity rights against the fake Kaun Banega Crorepati (KBC) lottery scams. In this scenario, Justice Chawla states "granted protection to the plaintiff, safeguarding the use of his voice, face, unique characteristics, and restrained the defendants from misusing his name. While determining whether a creation in question is infringing or not, there are multiple things taken into consideration.[24]" So, it's clear & evident that in India only under "Section 52 of the Indian Copyright Act," the concept of "Fair Dealing" where Deepfakes aren't exempting as Indian copyright jurisprudence[25] is very rigid and inflexible regarding "fair use.[26]"

Whereas in the USA fair use/ dealing laws have a fourfold examination which looks at the objective, the type of usage, the amount of original work employed, and the influence the material has on the market base. In a significant case, the US Supreme Court adopted the concept use,' which would readily accept any invention because Modernism implies the emergence of information has given new meaning and expression. Parodists use this as a defense against the transformational use of their creativity. Limits on these works will violation of free expression in the United States. Sensitive information requires more protection under the pretence of creative application.

Secondly in the USA the "Deepfakes Accountability Act, 2019" was passed ahead of the 2020 elections that mandated deepfakes watermarked for identification. Whereas in India Legislation isn't changing at the same rate as technology. At this point, India's technology law is inadequate to handle the concerns raised by AI algorithms.

Henceforth deep fake of Rashmika Mandanna observes that it shattered social media for that stringent Legislation required Delhi Police to file the case under the provisions of IPC & IT Legislations. Yet it is essential to make proper framework guidelines. To give a significant inception for the readers it's important to discuss one of the famous deepfake cases connected with personality rights.

[24] Face/Off: "Deepfake" Face Swaps and Privacy Laws | IADC, https://www.iadclaw.org/defensecounseljournal/faceoff-deepfake-face-swaps-and-privacy-laws/ (last visited Feb 8, 2024).

[25] Navigating Deepfakes in the World of AI – NLIU-CLT, (Oct. 11, 2023), https://clt.nliu.ac.in/?p=936 (last visited Nov 25, 2023).

[26] Applicability of section 52 of the copyrights act to specific works - Lexology, https://www.lexology.com/library/detail.aspx?g=6634c94d-77bf-40fb-8a56-e82da8067285 (last visited Nov 10, 2022).

As we know celebrities are becoming more careful in protecting their personality rights, which include their identities, speech, signatures, photos, and unique characteristics. In the famous case of Anil Kapoor, Personality Rights. Unfortunately, no specific statute addressing personal rights exists in India. They're ultimately found on a blend of legal precedents and guiding principles.

This case must now be exact in grasping the importance of strict consumer protection in deep fake marketing. In this scenario, Anil Kapoor is a Nineties celebrity known for his classic films. One of his films, "Jhakkas," is a parody; so, as a result, Anil Kapoor launched a lawsuit to preserve personal and privacy rights. [27]

In this case, famous film star Anil Kapoor witnessed the unauthorized use of AI technology to capitalize on his image, voice, and identity for financial benefits. The dilemma in the Copyright Law, arises how can legislation keep up with the constantly shifting ways that AI may change and share content? Copyright law may not be adequate to address circumstances in which AI-generated content duplicates a person's voice or likeness without their permission. Although Anil Kapoor tried to limit the use of his name, voice, picture, and memorable phrases in this case, it is evident that copyright law does not directly address the duplication of one's character using AI. Kapoor's issue, like the concerns of the musicians listed in the article, extends beyond the conventional limits of copyright protection, highlighting the need for a stringent legal framework. [28]

Finally, after critical analysis, the authors have found that exploring Personality rights, often known as the right to publicity or image rights, is an appealing option. It emphasizes that personality rights safeguard an individual's name, image, likeness, or other distinguishing features of their identity. Indian law recognizes an individual's right to manage and profit from their personality, which is frequently included in the wider context of the right to privacy.

By understanding the complexity of the issue that arose with his film name "Jhakkas" the Court delivered the verdict in favour of him. As technology has no boundaries it emphasizes the need for safeguarding public figures and personas from unauthorized profiteering and the misuse of AI technology. It does raise significant issues about the emerging environment of AI, privacy, and free expression. As technology advances, legal precedents such as this will become increasingly important in establishing the boundaries of individual rights and the obligations of those who generate the distributed digital material. Decision in the Indian legal system illustrates its adaptability of legislation or its dedication to preserving people's freedoms and reputation, despite the era of Artificial Intelligence.

---

[27] Rebalancing our regulatory response to Deepfakes with performers' rights - Mathilde Pavis, 2021, https://journals.sagepub.com/doi/full/10.1177/13548565211033418 (last visited Feb 8, 2024).

[28] Amisha Mittal, *Delhi High Court's Landmark Order: Protecting Anil Kapoor's Persona in the Age of AI – An Indian Legal Perspective*, THE IP PRESS (Oct. 9, 2023), https://www.theippress.com/2023/10/09/delhi-high-courts-landmark-order-protecting-anil-kapoors-persona-in-the-age-of-ai-an-indian-legal-perspective/ (last visited Nov 26, 2023).

Conclusion

Finally, the authors would like to comprehend by stating that Deepfakes are being widely used in creating content at an instantaneous rate. As a result, it is readily accessible to individuals owing to the emergence of AI. Though in India concept of "fair dealing" is there in Copyright Law certain issues still exist that require a stringent law as there's no viable technology available that can be effective in acting as an intermediary liability. The present regulations may not be sufficient to solve deepfake challenges using technology algorithms. There are concerns with regulating deep fakes, such as:

a. Deepfakes can be recognized and identified in real time.

b. Attribution shows, and the perpetrators are punished.

c. Owing to the difficulty in determining whether the material provided supports the concept of free speech or infringes one's right to privacy.

d. Ensure that the advantages to the victims are not overshadowed when pursuing these claims.

e. The influence of the courts' intrinsic time must be reestablished by the contemporary demand for deepfake control and mitigation.

f. Legal counsel must have technical expertise to undertake these forms of criminal allegations.

g. Remove the deep fake content from the internet as soon as possible.

These issues have long been argued in the field of cybersecurity. However, we as a community have a moral duty to minimize the spread of non-consensus harmful material. We've to educate ourselves and raise awareness about manipulations and the harm they may do. Youth should be taught about the implications of creating, posting, downloading, or spreading fraudulent information online. Regulators should prepare to embrace new approaches for controlling deepfakes so that the source of the content can be recognized and blocked appropriately. It is frequently observed that the primary argument used against bogus information is that an individual enjoys the freedom of speech and expression guaranteed by Article 19 of the Indian Constitution. We have to keep in mind that freedom of expression ends when one's right to privacy begins. Our responsibility here is to realize that our acts and freedom do not interfere with any other person's enjoyment of their rights. The right to withhold signature is a right guaranteed to every individual under Article 19 of the Indian Constitution, yet it cannot used to justify the creation and dissemination of fabricated or altered videographic content/still images that can manipulate people's thought processes regarding the content.

****