INDIAN JOURNAL OF LEGAL REVIEW

VOLUME 5 AND ISSUE 12 OF 2025

INSTITUTE OF LEGAL EDUCATION

INDIAN JOURNAL OF LEGAL REVIEW

APIS – 3920 – 0001 | ISSN - 2583-2344

(Open Access Journal)

Journal's Home Page – https://ijlr.iledu.in/

Journal's Editorial Page - https://ijlr.iledu.in/editorial-board/

Volume 5 and Issue 12 of 2025 (Access Full Issue on - https://ijlr.iledu.in/volume-5-and-issue-12-of-2025/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 73059 14348 - info@iledu.in / Chairman@iledu.in

INDIAN JOURNAL OF LEGAL REVIEW [IJLR – IF SCORE – 7.58]

VOLUME 5 AND ISSUE 12 OF 2025

APIS – 3920 - 0001 *(and)* ISSN - 2583-2344

Published by

Institute of Legal Education

https://iledu.in

"DEEPFAKES AND COPYRIGHT: NAVIGATING LEGAL LANDSCAPES"

AUTHOR – ADV.BINJU SIBY, DOCTORAL RESEARCHER AT CHRIST (DEEMED TO BE UNIVERSITY)

BEST CITATION - ADV.BINJU SIBY, "DEEPFAKES AND COPYRIGHT: NAVIGATING LEGAL LANDSCAPES", *INDIAN JOURNAL OF LEGAL REVIEW (IJLR),* 5 (12) OF 2025, PG. 544-555, APIS – 3920 – 0001 & ISSN - 2583-2344

ABSTRACT

Deepfakes, a revolutionary yet highly contentious application of artificial intelligence, have transformed the creation and manipulation of hyper-realistic media. These AI-generated fabrications blur the line between reality and fiction, posing significant challenges for copyright law and intellectual property rights. This article delves into the legal complexities surrounding deepfakes across four key jurisdictions: India, the United States, the United Kingdom, and the European Union. A key issue surrounding deepfakes is their copyrightability is whether AI-generated works possess the originality required for legal protection. Since traditional copyright law is founded on the principle of human authorship, the emergence of AI-generated content challenges existing legal norms. Determining ownership over deepfakes adds to this complexity, as multiple parties may be involved, including developer and the user. The lack of clear legal frameworks in many jurisdictions further complicates the enforcement of copyright laws, leaving gaps in protection and accountability for AI-generated media. Beyond copyright, deepfakes significantly impact personality rights, particularly regarding an individual's likeness, identity, and reputation. The unauthorized use of a person's image or voice, often for deceptive or malicious purposes, raises ethical and legal concerns. While some jurisdictions provide legal recourse for victims of deepfake misuse, others lack comprehensive protections. To address these growing challenges, legal reforms must balance innovation with accountability. Potential solutions include updating copyright laws to clarify AI-generated content's legal standing and strengthening personality rights to protect individuals from deepfake exploitation. A robust legal framework is essential to ensure responsible AI use while safeguarding intellectual property and personal identity.

Keywords: *Deepfakes, Copyright, Personality Rights, Fair Use, Fair Dealing, Artificial Intelligence, Authorship*

INTRODUCTION

The term Deepfakes is derived from the terms "deep learning" and "fake." It is a technology that uses the most advanced techniques of AI, such as GANs, to create very realistic yet entirely fabricated media. Deepfakes technology has been applied in entertainment, education, and healthcare and promises innovation and efficiency. Its misuse for disinformation, revenge pornography, and fraud pose very serious ethical and legal dilemmas. Recently, this sophisticated deepfake technology emerged as one of the powerful tools that can create very realistic audio, videos, and images, capable of printing on the appearance, voice, or actions of real people. Large variety of possibilities were thus created in entertainment, art, and communication while raising very serious concerns about such misuse. Such precision in the manufacturing of content raises complex identity, privacy, and intellectual property issues. It was in these interests that copyright law was conceived to protect creators' rights over original works, putting it in relatively uncharted waters by trying to come to terms with the digital era where deepfakes complicate issues of authorship and originality. Since deepfakes often include some form of transformation of already-created media, for example video clips, images, or sounds, questions arise pertaining to rights; who owns the rights to the new version of the work? Should an original creator have dominion over the work or does the producer come into a newly created ownership over his work? These emerging issues hence compel legal systems to rethink how copyright law could deal with the intricacy of digital manipulation as a way of protecting creators and preventing abuse at the same time. This paper shall explore such jurisdictions' attempts at answering the challenges by concentrating mainly on the copyright law, authorship attribution, and intellectual property rights enforcement.

DEEPFAKE TECHNOLOGY OVERVIEW

Deepfakes can alter or create completely new outputs in visual, audio, or textual content. Some of the most common ones are:

- **Face Swapping**: Replacing one person's face with another's in images or videos.
- **Audio Dubbing**: Audio accompaniment matching lip movements in video, making False Speech.
- **Puppet Techniques**: Manipulating a subject's movements or expressions, creating situations or conversations from scratch.

Creation process

Deepfakes are based on Generative Adversarial Networks and encoder-decoder models.[846] The algorithms study vast collections of real-world media in order to generate synthetic images, audio, and videos with incredible accuracy resembling real people[847].

Emergence and speed

The technology behind deepfakes has become radically easy to use, from cloud-based services to mobile applications, such as Zao and Deepfakes Web, which empower a common user to create and further distribute deepfakes.[848]This growing accessibility has unlocked creative and educational possibilities, allowing people to experiment with storytelling, simulation, and digital innovation in entirely new ways.

However, this powerful technology also brings with it serious concerns that cannot be overlooked. Deepfakes have been misused to infringe copyright, violate individuals' privacy by manipulating their likeness without consent, and cause significant reputational harm. The emotional and social consequences for individuals targeted by malicious deepfakes can be deeply damaging, especially when such content spreads rapidly across digital platforms.

These risks highlight the urgent need for clear and responsive legal frameworks that can keep pace with technological change. Beyond just regulation, what is needed is a thoughtful, human-centric approach—one that encourages innovation while ensuring people are protected from misuse. As we move forward, striking this balance will be essential to fostering a digital environment where creativity thrives without compromising individual dignity and trust.

Though the scope of creative and educational applications is limitless, deepfakes have associated risks such as copyright infringement, breach of privacy, and reputational damage, which calls for robust legal frameworks and innovative enforcement mechanisms.

COPYRIGHTABILITY OF DEEPFAKES

The rise of Deepfakes has led to talk about the copyrightability of this kind of material, as well as its 'Creator'[849]. Inasmuch as the material itself is computer-generated, the term 'Creator' has been construed to have at least two meanings.

[846] Hrisha Yagnik, Akshit Kurani and Prakruti Joshi, 'A Brief Study on Deepfakes' (2020) 075

[847] Aranya Nath & Sreelakshmi B., Deepfakes on Copyright Law - Inadequacy of Present Laws in Determining the Real Issues, 15 INDIAN J.L. & JUST. 285 (March 2024

[848] Shriya Sayanak, A Study on Deepfakes and Copyright Infringement, 6 INT'l J.L. MGMT. & HUMAN. 3541 (2023).

[849] Akhtar Hussain, Deep Fakes: A Challenge to Copyright Law, 3 JUS CORPUS L.J. 249 (June 2022).

1.The deepfake program must be developed by an individual.

2. A user of an existing work to realize his or her dream.

Some thinkers are of the view that AI systems, in themselves, do not have rights as human inputs are always essential for their proper working. The Supreme Court of the USA has outrightly ruled that copyright protection arises only in situations of genuine originality of works created by human minds. Computer-generated works', is the definition under copyright in the UK as provided for the items created by Artificial Intelligence. According to the CDPA[850] Act 5 Section 178: a work whose content is entirely generated by a computer without any human contribution would fall within that category. This is clearly on the side of Deepfakes as they inherently fall within this definition of being produced by AI work[851]. The section 9(3)6 of the Act provides that an author is that person who provided the condition to produce such a work. Under the case on consideration, it has been well described by the High Court of India that the copyright lies with those who are producing works owing to their skills and effort. However, recently, some developments have also come in India for acknowledgment of AI authorship rights in artistic creation[852]. 'Suryast' a painting made by RAGHAV,8[853] 'an AI program was filed with Ankit Sahni as co-author and copyright holder. This was on the grounds of an Adopted Resolution that argues that if there is a little bit of human input in the creative process, then AI-created works could be copyrightable. Clearly, it's a question of law concerning copyrightability regarding Deepfakes content, differing in various jurisdictions. In some countries, creativity forms the basis of copyright, while in other countries, AI's contribution to the creative process is recognized only in certain instances. As the technology for AI developed, over time, the systems needed to evolve and also clarify the rights and liabilities associated with the contents produced by AI.

COPYRIGHTABILITY OF DEEP FAKES IN DIFFERENT JURISDICTIONS

Legislation surrounding deepfakes often overlooks the copyright implications. Some may mistakenly assume that existing copyright protection can be used to combat deepfakes. However, it's important to note that copyright laws, in different jurisdictions, don't always protect against deepfake violations.[854] In this study, we delve into the concept of 'fair use' as outlined in the US Digital Millennium Copyright Act 1998 as well as 'fair dealing' under the Indian Copyright Act of 1957 and the UK CDPA Act 1988. By exploring these approaches, we aim to understand how copyright law addresses the challenges posed by this disruptive technology.

INDIA

Copyright Act, 1957:

The Indian Copyright Act 1957 (ICA) 21 defines fair dealing at Section 52, which determines what works are exempt from being treated as copyright infringement. Unlike the United States, fair dealing in India is regarded as an exception to copyright infringement. The law provides a list of acts that are not infringements. Such an approach may be termed rigid by some. The approach works well with created deepfakes because a use like this does not come under any of the acts contemplated in Section 52 of ICA.[855] However, this provision will not protect the use of deepfake technology. Indian judicial authorities have begun to adopt the meaning attributed to the word 'review' as defined in Section 52(1)(a)(ii) of the Indian Copyright Act. Recently, this trend is seen in modern cases such as those of the University of Oxford v Narendra Publishing House ILR (2009) 2 Del 221[856]. In this case, the courts illustrated the principles which will apply in order to safeguard

[850] Copyright and designs act 1988
[851] ibid
[852] 4 Jackie Snow, 'Deepfakes for Good: Why Researchers Are Using AI to Fake Health Data' Company, 24 September 2018) accessed 21 October 2022.
[853] Sukanya Sarkar, Exclusive: India recognises AI as co-author of copyrighted artwork
'India Recognizes AI as Author of a Copyrighted Work' (Lex Campus, 11 August 2021)

[854] ibid
[855] Indian copyright act 1957, sec 52
[856] University of Oxford v Narendra Publishing House ILR (2009) 2 Del 221

classes of work that represent social values embedded in works. Moreover, on questions of usage, Indian judicial precedents are generally to be found in reports and thus don't extend into the context of deepfakes at issue in the present case. Section 57 of the Indian Copyright Act[857] thus confers, inter alia, a basket of rights including the right of integrity as determined by the Berne Convention, 1886. It goes without saying, therefore, that the right of integrity as explained in Section 57(1)(b) of the ICA applies to the phenomena known as deep fakes and hence can be classed as distortion, mutilation, or other alteration of any work of some individual. The rights of the authors under the statute include keeping their rights over their creations such as reproduction, publication, and public exhibition. Sections 55[858] and 63 of the Indian Copyright Act elaborate on the penal liabilities that come along with the copyright infringement along with the available remedies such as damages, injunctive relief, imprisonment, and a range of fines for the person concerned.[859] Section 51 states that all acts performed without permission shall carry penal consequences, which in turn makes deepfakes liable to breach of copyright. The landmark case of Amarnath Sehgal v. Union of India 17(2005)DLT717, 2005(30)PTC253(DEL) [860] was the first case wherein the moral rights of an author were held to be applicable with the intent of their works not being altered or diluted.

Information Technology Act, 2000: The act provides specific provisions for digital offenses. Section 66D[861] deals with identity theft and impersonation.[862] Section 67 criminalises transmission of obscene or explicit material, which may be some sort of deepfakes. Section 79 of the Information Technology Act, 2000, or IT Act deals with intermediary liability applicable for copyright infringement following Myspace Inc. v Super Cassettes Industries Ltd. , (2017) 236 DLT 478 (DB), [863] Judgment, The Delhi High Court interpreted the provisions of the Indian Copyright Act and the Information Technology Act in a way that makes intermediaries liable for the removal of infringing content upon notification from private parties, even without a judicial order, particularly in copyright infringement cases. Yet, the detection of deepfakes remains a serious challenge, albeit one due to technological limitations and hence makes intermediaries' job of implementing the content moderation policy regarding the takedown of deepfake content cumbersome.

UNITED STATES

The U.S. legal system grants copyright protection but does have challenges in the exercise of these rights concerning AI-generated deepfakes. Under US law, the doctrine of fair use is granted latitude and is protected under Section 107 of the Copyright Act of 1976.

It encompasses the following tests which consider the following factors.

1.The nature of the use

2.The nature of the work

3.The volume and quality of the work; taken

4.The impact on the market place. The doctrine of fair use has a field more than fair dealing.

Deepfakes are used for purposes different from those intended for the original work.[864] The majority of the cases pass the purpose and character test of the fair use doctrine. Furthermore, U.S Courts have been established directly to hold that if the purpose of the usage falls in the category of 'transformative' if there is the copyrighted material or in cases where a good deal borrowed from another work may be involved it qualifies as fair use. In Jay-Z v. Deepfake Creators, courts have addressed the unauthorized use of the artist's voice in audio deepfakes by holding creators liable for

[857] Indian copyright act 1957

[858] ibid

[859] Aranya Nath & Sreelakshmi B., Deepfakes on Copyright Law - Inadequacy of Present Laws in Determining the Real Issues, 15 INDIAN J.L. & JUST. 285 (March 2024).

[860] Amarnath Sehgal v. Union of India 17(2005)DLT717, 2005(30)PTC253(DEL)

[861] Information technology act 2000

[862] ibid

[863] Myspace Inc v Super Cassettes Industries Ltd, (2017) 236 DLT 478 (DB),

[864] ibid

infringement and misuse. In the case of Bill Graham Archives[865], the United States Court of Appeals, for the Second Circuit said that when a copyrighted work is used in a manner that differs from its expressive purpose it is excusable. Similarly, in this context, given the fact that this technology is still in its early stage and has little market value, it does not pose a significant threat to the market of original creations. This requirement is also satisfied[866]. As a result, in the United States, copyright laws allow content creation to be considered as fair use. However, these laws fail to make a distinction based on the intent of the creator; this means deep fakes might fall under parodies and are, therefore, protected. Several states in America have proposed bills that would help systematically eliminate the cases where replicas and other forms of actions relating to the portrayal of people and happenings are made. Another related issue in this context is pornography.

Legislative Measures: Focused efforts at the federal and state levels target the specific abuses of deepfakes[867]. At the federal level, the Deepfakes Accountability Act requires that watermarked altered content be used; California and Texas specifically outlaw the use of deepfakes in elections and revenge porn; and Virginia is leading in amending the law to include provisions for the treatment of content classified as 'Falsely created material'.

UNITED KINGDOM

The UK Copyright, Designs, and Patents Act, 1988, generally forms the legal basis under which copyright cases on deepfakes are managed. More particularly, Section 29 and Section 30 form some exceptions of the general rule surrounding copyright. Generally, such provisions are for safeguarding use based on permission obtained from the copyright holder and not granted or sought at that particular point. Provisions are applicable to three situations: research or private study for the purpose of criticism/ review as well as reporting on current events. There is no statutory definition under the UK statutes of fair dealing as to what may be fair.[868] In Hubbard v Vosper [1972] 2 QB 84[869] Lord Denning said that 'fair dealing' cannot be precisely defined and is fact sensitive. This was the attempt of the judiciary to devise a test to decide fairness as fair dealing cannot be defined. Since that time, other considerations enter the picture: the nature of the work-how it was obtained, the extent of its use, the character and purpose of the use, whether it has any implications, the motive for its use, the effect on the works market value, and whether there were alternatives that were non copyrighted. Fair dealing also provides protection to such works created as parody, caricature, or pastiche under Section 30A14, 'Schedule 2 (2A) of the CDPA'[870].The case in the UK has seen various criticisms as against the stringent approach and rigidity in handling when such a flexibility exists in handling the deepfakes. Those deepfakes created for purposes may be protected, for example, if used in research or as a means of expression. This problem was determined by the Civil Division of the Court of Appeal, in England and Wales in Hyde Park Residence Ltd. and Yelland & Ors [2000] EWCA Civ J0210-2[871] relying heavily on the motive of an alleged infringer in a fair dealing issue which does come into play when there is the production of deepfakes made in bad faith.

EUROPEAN UNION

The European Union has taken head-on the issues of deepfakes with a very active and integrated approach to address the problem on

[865] Bill Graham Archives v. Dorling Kindersley Ltd , 448 F.3d 605, 615 (2nd Cir. 2006)

[866] 4 Jackie Snow, 'Deepfakes for Good: Why Researchers Are Using Al to Fake Health Data' Company, 24 September 2018) accessed 21 October 2022.

[867] Akhil Satheesh, Deepfakes and the Copyright Connection: Analysing the Adequacy of the Present Machinery https://jolt.richmond.edu/2022/01/25/deepfakes-and-the-copyright-connection-analysing-the-adequacy-of-the-present-machinery/accessed on 20 october 2024

[868] Alexandra Atsüren,EU Strengthens AI Regulations and Targets Deepfakes Amid Rising Concerns https://www.bioid.com/2024/06/03/eu-ai-act-deepfake-regulations/, accessed on 20 october 2024

[869] Hubbard v Vosper, [1972] 2 QB 84

[870] Copyright, Designs, and Patents Act, 1988

[871] Hyde Park Residence Ltd. and Yelland & Ors [2000] EWCA Civ J0210-2

issues like privacy, security, and the general public debate. Indeed, given the fast-changing pace of such emerging technology, EU lawmakers realized they need a strategy to be all things to the multifaceted requirements, bridging the approach from regulation by rules and tech-based solutions with respect to a proper response. An important piece of this new model is, therefore, the Digital Services Act, or DSA. The DSA has come into force in 2022. In essence, the DSA increases the responsibility of the digital platforms with respect to handling illegal content; for example, deepfakes, and should ensure transparency into how such content is managed. Online services are also required to provide users with mechanisms to report harmful content, such as synthetic media, and ensure that manipulated content is marked in a way that is clearly distinguishable from authentic media.

At the same time, the AI Act, launched in 2021, addresses high-risk applications by specifically defining them as those, such as deepfakes, which have a significant impact on the operation of the digital environment. The AI Act has regulatory requirements to establish standards for high-risk AI systems. It should ensure transparency, accountability, and oversight. Deepfakes must be disclosed under the Act: AI-generated content, such as synthetic images or videos, that should be so identified to consumers, protecting against deceptive or misleading representations. Another direction of the AI Act is related to preventing uses of AI that can breach privacy rights. It encompasses an essential issue related to interaction with biometric data, such as when such AI systems use facial recognition, which is popular in deepfakes[872].

Deepfakes, by definition, are serious issues under the General Data Protection Regulation, which is essentially a framework in the EU protecting personal data[873]. The GDPR focuses more on the rights of the individual to their personal data and control, such as having the right to consent over the use of one's likeness, voice, or image. In most cases, deepfakes are associated with an unauthorized use of these personal attributes, which could be a potential breach of the explicit consent required by the GDPR. A deep fake that involves an abuse of some person's identity without permission will be considered violating their data rights, and one may be able to get such remedies as being forgotten or the right to be erased. It is such that one can get his/her information erased from several online applications, and in many cases, it uses one's data.

Following these principles, the EU has mainly acted towards the end of removing misinformation and false reports. Deepfakes form one area within this extensive realm of mayhem. Deepfakes are used to undermine public opinion, cheat voters, or harm the integrity of public personalities. The European Commission addresses this situation as it ensures an action plan to fight the growing risk of disinformation, while focusing much on deepfakes. The Code of Practice on Disinformation is a participative industry initiative nudging platforms to be more responsible by the measures they undertake to identify, label, and minimize the effects of harmful content, which includes deepfakes. To this end, platforms are also under pressure to educate users on the risk of manipulated media and how they can improve their media literacy, thus enabling the public to critically evaluate what they are consuming[874].

The EU is responding to the deepfakes phenomenon through research and technology-based solutions focused on the detection and prevention of media misuse produced by AI. For instance, Horizon 2020 Program is used to finance projects in the research areas of AI and cybersecurity and technologically advanced deepfake detection. These projects are working on the development

[872] 4 Jackie Snow, 'Deepfakes for Good: Why Researchers Are Using AI to Fake Health Data' Company, 24 September 2018) accessed 21 October 2022.

[873] Aranya Nath & Sreelakshmi B., Deepfakes on Copyright Law - Inadequacy of Present Laws in Determining the Real Issues, 15 INDIAN J.L. & JUST. 285 (March 2024)

[874] ibid

of more effective tools for identifying manipulated content, which would be used by law enforcement, regulatory bodies, and digital platforms to quickly and accurately detect deepfakes. The EU is also exploring ways to develop standards and certifications for verifying the authenticity of digital content, ensuring that users can trust the media they encounter online.

Thus, while the EU's regulatory and technological efforts thus far have provided an excellent base upon which to handle the risks related to deepfakes, it is also coupled with various challenges. This is because, due to its global nature, the internet tends to allow content to cross borders easily, complicating the tasks of enforcement and regulation. The EU has called for increased international cooperation and the development of global standards to address the cross-jurisdictional nature of deepfake distribution. As deepfake technology continues to evolve and improve, regulatory frameworks must be adaptable and continually updated to keep pace with these advancements**.**

PERSONALITY RIGHTS AND DEEPFAKES

Personality rights are legal protections that safeguard an individual's identity, including their name, image, voice, and other personal characteristics, ensuring that they have control over the commercial use of these attributes.[875] These rights are particularly important for celebrities, whose public image often plays a crucial role in their career and livelihood. It is along this line that personality rights earned a place in the Indian intellectual property laws, all the more in the wake of landmark cases Auto Shankar AIR 1995 SC 264, (1994) 6 SCC 632[876] and Anil Kapoor vs. Simply Life India & Others Anil Kapoor v. Simply Life India, 2023 SCC OnLine Del 6914[877] which opened the grounds to defend celebrity persona in Indian law. The Auto Shankar case outlined the importance of recognizing a person's right to control the commercial use of his identity, while the Anil Kapoor case was an extension that dealt with unauthorized use of the image of a celebrity in deepfake videos and merchandise and was held to have violated the personality and publicity rights of the actor. In this regard, it is very nasty how the wellbeing of income, reputation, and public image of a celebrity may be affected through deepfakes.

Deepfakes are AI-driven manipulations of video, audio, or images, and this is a major challenge for personality rights[878]. This can create extremely realistic but absolutely fabricated media in a way likely to mislead the public or exploit a celebrity's identity without permission. Deepfakes can be used, for instance, in commercial exchange in the sense of false endorsement or association which is a damage to celebrity repute or cause emotional distress in putting the person into misleading or scandalous contexts. Those are uses that run afoul of the right of publicity because it deprives the individual of control over use of the likeness of the individual[879].

For example, consider the face of a movie actress like Rashmika Mandana which is superimposed onto some other body, utilized in porn sites, and it was posted by publishing that in the same pornography site, there by invading the publicity right with defamation for the face-artist. Another example is kim Kardashian[880], where Vogue was able to delete a deepfake of Kim Kardashian from a site where the deepfake had made use of materials from a video by Vogue.

Challenges in Copyright Enforcement

Many challenges come in enforcing copyright over deepfakes, including the following:

[875] Nashyam Saadiya ,Protecting Personality Rights In India,https://www.mondaq.com/india/privacy-protection/1475772/protecting-personality-rights-in-india,accessed on 27 october 2024

[876] R. Rajagopal & Ors. vs. State of Tamil Nadu & Ors.

[877] Anil Kapoor v. Simply Life India, 2023 SCC OnLine Del 6914

[878] 2Belinda Scrimenti, 'Using AI to replicate the voice of a celebrity – Watch out for Legal issues Including Violating the Right of Publicity' (Broadcast Law Blog, 04 April 2023) accessed 24 September 2023

[879] Sudharsan S. Sri, *AI and Personality Rights: Legal Implications*, 6 INT'l J.L. MGMT. & HUMAN. 2278 (2023).

[880] Tiffany C LI, Kim Kardashian v. Deepfakes, SLATE (June 18, 2019)

1. Technological challenge: It is hard to detect deepfakes because of their rapid developing[881] technology, thus it becomes increasingly complex and realistic. The more intricate deepfake algorithms, the better it can simulate human features, voice patterns, and movements and is therefore harder to identify whether content is altered or authentic media. This technological advancement is much more than the evolution of detection tools that could not keep up with the complex and subtle changes developed in the more advanced deepfake models.

The uncertainty regarding deepfakes directly correlates to copyright and other rights protection. For instance, determining whether the content is a deepfake or the original source of the infringement can only be determined by the aid of advanced tools and technical expertise. Besides, the latest deepfakes are precise to the point that evidence of manipulation can no longer be trusted in proving cases of unauthorized use or intent. Most likely, the alterations made for deepfakes are less or, in the best case, for purposes of gray area legislation, which may be parody or satire.[882]

The final roadblock is that there is no detection mechanism that is dependable and available to all. This affects the response of regulatory authorities, courts, and platforms to deepfake-related copyright infringement. The misuse opportunities lie in the gaps as offenders exploit these gaps to evade accountability. Thus, there is an urgent need for continuous investment in advanced detection technologies and standardization of protocols for the identification and authentication of digital content. These will not only increase the capabilities for enforcement but will also significantly strengthen protections to creators, individuals, and entities from deepfake technology misuse.

2. Fair use and fair dealing. There are differing jurisdictions with significantly different interpretations regarding the 'fair use' and 'fair dealing' exceptions on copyright infringement and hence make it inconsistent as to how deepfakes are to be regulated and enforced. The United States applies a wide and open exercise of a doctrine of fair use, while this court takes into consideration factors for purposes and character of use, the nature of the original, amount used in comparison to the work as a whole, effect on the market for the original material, and more. And under such an approach accommodating creative interpretation, it quite regularly discovers transformative purposes of use or additions of some new meaning and context to originals. For instance, in the case of Bill Graham Archives v. Dorling Kindersley Ltd , 448 F.3d 605, 615 (2nd Cir. 2006)[883], a court decided that copyrighted images might be used within a book for the simple reason that they had transformative quality but did not do any harm to the market for the original works.

Fair dealing' is much more circumscribed in countries such as the UK and India and has limited purposes: for instance, for the purposes of research or criticism or review. With tighter bounds, it means any uses that are outside of the above-mentioned categories will more likely be deemed to infringe. In Hyde Park Residence v. Yelland[884], the UK court dismissed a fair dealing defence for the use of photographs from a video, noting that the purpose was not among the permissible under the fair dealing exceptions.

With deepfakes, these disparate interpretations can mean inconsistent enforcement. In the United States, for instance, such a deepfake would likely qualify as a fair use protection as a transformative work particularly in the exercise

[881] Danielle F. Bass and Nathaniel Penning , The Legal Issues Surrounding Deepfakes https://www.honigman.com/the-matrix/the-legal-issues-surrounding-deepfakes, accessed on 2 november 2024

[882] Sashwat Kaushik,understanding copyright issues entailing deepfakes in india, Understanding copyright issues entailing deepfakes in India - iPleaders, accessed on 4th November 2024

[883] Bill Graham Archives v. Dorling Kindersley, Ltd.448 F.3d 605, 615 (2nd Cir. 2006)

[884] Hyde Park Residence Ltd v Yelland & Ors | [2000] RPC 604

of parody, comment, or otherwise transformative works[885]. The UK and India could however interpret the very same deep fake to infringe on someone's rights absent clear classification in the stricter exceptions of fair dealing. It generates confusion across the different borders of an increasingly borderless digital space since deepfake content moves fast across such international borders. Additionally, it brings to the fore how intellectual property rights need to be balanced with incentives so as to spur innovation and creative expression. Such imbalances will therefore call for international cooperation and probably for the harmonization of copyright exceptions to make for more uniform regulation of such new technologies as deepfakes.

3. Moral rights: The moral rights are the rights which protect the author's right to attribution and ensure that the work is not distorted, mutilated, or otherwise modified in derogatory form. They are particularly relevant in discussions on deepfakes. These rights are recognized by the copyright laws of the UK and India, which emphasize the personal and non-economic connection between creators and their works. However, the application to the case of deepfakes remains a contentious issue, with AI-generated media creating new considerations. Moral rights in UK copyright law include the right to be identified as an author and the right to object to derogatory treatment of a work[886].

The Indian copyright law further confers rights upon authors with regard to authorship and seek remedies if the work done by them is distorted or misused in a manner prejudicial to their reputation, under Section 57 of the Copyright Act 1957. The application of these principles would then succeed to afford some protection where the image, voice, or identity of a person has been manipulated and used against his or her best interests in order to harm the person's reputation or falsely suggest an association with a work[887]. And herein lies the issue with deepfakes-the distinction between creation and unauthorized copy collapses. The fact that most deepfakes are made through AI and, combined with the element of not directly using the copyright work, makes this concept fuzzy about moral rights. For example, a creator may claim there is infringement of moral rights in a deepfake when the original work of an author or artist is being used in a misleading manner. However, it remains questionable when such an application of moral rights will arise when an individual's identity or likeness is manipulated by a deepfake, without any causal link to some particular copyrighted work. The further development of the technology and how it can make entirely new works by piecing together fragments of data makes this enforcement of moral rights even harder. This has led to debate about whether this necessitates modifying the existing copyright regime to suit such eventualities. Whereas rights in respect of reputation may help establish the boundaries around protection offered by these rights to the authors and individuals against reputational harm, the extension of this right to cover abuse of personal identities through deepfakes will probably require amendments to the legislations and judicial interpretation effectively to protect it in this new area.

4. International harmonization: The lack of international harmonization concerning the deepfakes on copyrights has led to a disparate legal landscape. This inconsistency makes it difficult for enforcement regarding copyrights and more sharply across national borders, cross-border deepfake content. Since the development and sharing of the content would be transmitted freely on the web and at very low costs in the world, deepfakes often pose complex measures to combat the infringement of the rights for the IP. Because protection mechanisms vary country by country especially relating to the digital media-related rights such

[885] ibid

[886] ibid

[887] Indian copyright act 1957, section 57

as rights of personality or unauthorized use of a celebrity's image, uniform and stern action cannot be taken against the deepfakes. For instance, while some countries have very harsh privacy and personality rights laws; others do not have them, and thus a deepfakes creator can download content without retribution.

And copyright law, which differs in its views of some questions such as fair use, right to commercial exploitation, and right to protection for a digital identity. The process of law enforcement becomes cumbersome without an international framework coherent and standardized regulation in place when deepfake content crosses borders. This bars celebrities, public figures, and other content creators from adequately protecting their intellectual property because remedies may not be available or are radically different in the jurisdictions. As such, there is a vast need for international cooperation and harmonization in formulating laws that can counter the challenges of deepfakes and ensure a uniform approach toward copyright internationally.[888]

5. Intermediary Liability: Hosting platforms have to put huge pressure on identifying and moderating deepfakes. Deepfakes are difficult to detect with evolution, and they spread instantly across social media and other internet platforms before action is taken by moderators. This puts any user-generated content host in an odd bind: free speech must be preserved, but bad speech, or otherwise deceptive/infringing, needs to be removed from the page sooner rather than later. This principle is reflected in such famous cases as Myspace Inc v Super Cassettes Industries Ltd, (2017) 236 DLT 478 (DB),[889]. In this case, the court held MySpace[890] liable for failure to act swiftly enough to remove infringing content once it had notice of the existence of infringing content. This case underlines the vigilance that must be shown by platforms in response to complaints so that they are in compliance with the law as it applies to the removal of infringing content and protection of rights owners.

FUTURE DIRECTIONS

The legal and regulatory landscape surrounding deepfake technology is evolving rapidly, as governments around the world begin to address the complex challenges posed by this powerful and increasingly accessible form of synthetic media. With deepfakes becoming more sophisticated and easier to create, legal systems are under growing pressure to respond effectively. Legislators are now re-evaluating outdated legal provisions and proposing targeted reforms to ensure that regulatory frameworks are aligned with the realities of today's digital ecosystem. The core objective is to maintain a careful balance—one that encourages innovation in artificial intelligence while safeguarding individuals and society from the misuse of such technologies, particularly in areas related to privacy, reputation, consent, and the spread of misinformation.

In the United States, legislative momentum is building around the regulation of deepfake content. Federal authorities are considering new laws specifically designed to curb the proliferation of deepfake pornography and synthetic media that facilitates the spread of disinformation. On the state level, Virginia has taken the lead by enacting a statute that explicitly criminalizes the nonconsensual distribution of deepfake pornography. These developments highlight a growing recognition of the need to hold individuals accountable for malicious uses of synthetic media, and to ensure that victims have legal recourse in both civil and criminal contexts.

India is also taking proactive steps by proposing amendments to its Information Technology Act. These reforms aim to establish clear liability for the harmful use of deepfakes, particularly in cases where such content is used to malign reputations, distort public perception, or disseminate false narratives. This legislative effort responds to a noticeable rise in deepfake-related incidents within the country's digital

[888] ibid
[889] Myspace Inc v Super Cassettes Industries Ltd, (2017) 236 DLT 478 (DB),
[890] https://www.bananaip.com/super-cassettes-industries-v-myspace/

space, many of which have had serious personal and societal consequences. The proposed amendments underscore India's intent to build a regulatory framework that is both responsive and preventative in nature.

The United Kingdom faces a more intricate challenge: integrating deepfake regulation within its established copyright system, which already includes fair dealing exceptions. As policymakers consider new legal instruments tailored to AI-generated content, there is a concerted effort to ensure that these regulations do not impede creative expression or technological development. At the same time, the UK seeks to reinforce protections for copyright holders and uphold the public interest—especially as AI becomes an increasingly prevalent tool in media, art, and research.

At the international level, coordinated action is emerging as a necessary component of any long-term solution. The World Intellectual Property Organization (WIPO), among other global bodies, is actively engaging with member states to foster dialogue and propose harmonized frameworks for addressing deepfake-related challenges. Such international cooperation is crucial, given the inherently cross-border nature of digital content and the global reach of synthetic media. By establishing common legal standards and promoting collaborative enforcement mechanisms, the international community can better manage the risks associated with deepfakes while enabling their constructive uses.

The global response to deepfake technology is moving toward a more structured and principled approach one that emphasizes legal clarity, technological adaptability, and cross-jurisdictional coherence. This evolving framework reflects a broader commitment to ensuring that innovation in artificial intelligence serves the public good without undermining fundamental rights and social trust.

CONCLUSION

This research article critically analyses the challenges posed by deepfake technology to copyright law across three major jurisdictions—the United States, India, and the United Kingdom. With the increasing sophistication of deepfakes, powered by machine learning algorithms, the legal implications of impersonation and the manipulation of reality have become more pressing. While deepfakes hold potential for creative, educational, and research-driven applications, they also present risks of copyright infringement, misappropriation of identity, and reputational harm. In the United States, the copyright framework is guided by the doctrine of fair use, which permits transformative uses of copyrighted content under certain conditions. Although this flexibility supports innovation and freedom of expression, it has been criticized for providing legal cover to harmful or malicious deepfakes, particularly where intent is difficult to assess. This creates challenges for regulators and platforms attempting to moderate such content effectively. India, by contrast, follows a more restrictive fair dealing approach. Here, specific exceptions are outlined under which copyrighted material may be used without constituting infringement. Indian jurisprudence places considerable weight on the intention behind the creation of content, thereby offering safeguards against misuse. However, this approach tends to overlook or inadequately support the legitimate and beneficial uses of deepfake technology for purposes such as education, satire, or artistic expression. The United Kingdom adopts a relatively balanced approach, factoring in both the purpose and the intent behind the creation of deepfakes. This allows for lawful use in contexts such as parody, research, and commentary, provided there is no malicious objective. Nonetheless, even this model faces difficulty in addressing the growing complexity and scale of deepfake content in the digital age. In light of these comparative insights, the article underscores the need for a nuanced, flexible, and technologically informed legal framework. Such a framework should be capable of distinguishing between malicious and legitimate uses of synthetic media while ensuring robust protection for original creators. It should also facilitate the socially beneficial applications of deepfakes, particularly in areas like education, cultural expression, and public interest communication. Equally important is the development of reliable deepfake detection technologies that complement legal efforts. These tools can support content moderation, evidence gathering, and enforcement, thereby strengthening regulatory responses to harmful content. Ultimately, the legal response to deepfakes must be multidimensional, integrating legislative clarity, technical innovation, and cross-sector collaboration. Only through a holistic and adaptive approach can the challenges of deepfake technology be effectively managed while encouraging its responsible and constructive use.