COPYRIGHT LAW AND INDIA: THE DEEPFAKE PROBLEM

Aayush Kaushik, B.B.A. LL.B. (Hons), Jindal Global Law School, O.P. Jindal Global University, Sonipat, Haryana

ABSTRACT

With the rapid development in technology and the advent of generative AI, there has been a contrast with the development of legislation. Intellectual Property Rights have always been a murky area of law, however, with the ever-growing disparity between technology and legislation, the hurdle of identifying what is real and what is fake is becoming difficult with each passing day. Since it is a new concept, there is a dire lack of literature and jurisprudence on the subject is still in its infancy.

The first part of the paper will analyze what deepfakes are and whether we need a separate law to regulate them. It will also go into the critical issue of ownership regarding such content, particularly whether it belongs to the creator of the deepfake or the individual whose likeness has been used.

The second part will analyze how countries like the USA, which have been pioneers in the arena of IPR, are tackling the issue of regulation of deepfakes. It will also address whether there is a solution without the involvement of law that can help tackle this issue.

The third part of the paper will focus on how the European Union has approached this problem. The EU has had very stringent laws regarding the use of data and has always had a consumer-centric approach, hence its views on the regulation of deepfakes and the issue of who owns the content are crucial to the overarching debate regarding generative AI.

Lastly, the fourth part of the paper will analyze India's standing in this whole scenario and what India can learn from the mistakes of other nations. It will see what Indian jurisprudence can borrow from these international models by molding it according to India's requirements.

Part 1: The DEEPFAKE problem!

The use and development of generative AI have ballooned in recent years, so much so that it has outpaced existing regulations aimed at safeguarding against the use of malicious or unethical practices[1]. One of the most prominent uses of generative AI is deep fake content, which has caused widespread concerns. So, what actually is a deep fake? While deep-learning AI has the ability to recognize things, they still do not have the ability to create them. Generative Adversarial Networks or GANs were developed to remedy this problem as it gives machines something akin to imagination, allowing them to create content from scratch[2]. Deepfakes are lifelike audio or video that have been generated using these GANs based on the prompts given to a computer. It involves superimposing someone's face onto another person's body in a way that appears genuine. Computer software examines several photos and videos of the target person's face to determine its characteristics and expressions. Then it utilizes this information to generate a new video or picture in which the target individual seems to say or do things they never did. This is just one area in the complicated realm of AI that lawmakers are trying to decode.

With the arrival of ChatGPT, AI has become mainstream, enabling the creation of ever-more realistic deepfakes a cup of tea. This has raised some serious questions: Who is the owner of deepfake content- the person who created the content or the one whose likeness has been used? And, more importantly, is there a need for deepfakes to be regulated?

Coming to the first question of who the owner of such AI-generated content is- the person who created the content or the person whose likeness has been used to make the content. It is important to identify the true owner of the work to hold them accountable if the content produced by them is of malicious intent. While such a question is yet to come before the court, we can delve into the nuances of already existing jurisprudence to find an answer. Intellectual property by definition means something that a person or persons have created using their intellect or a creation of minds, hence the true owner of deepfake content should be the person who actually created the content using the likeness of another person(s). This is because the

[1] Aled Owen, 'Deepfake laws: Is AI outpacing legislation?' (*Onfido,* 2 Feburary 2024) <https://onfido.com/blog/deepfake-law/>

[2] Martin Giles, 'The GANfather: The man who's given machines the gift of imagination' (*MIT Technology Review*, 21 February 2018) <https://www.technologyreview.com/2018/02/21/145289/the-ganfather-the-man-whos-given-machines-the-gift-of-imagination>

person who created the content, for instance, the AI-generated song of Drake and the Weeknd, used their intellect to create a voice model of the two singers and then generate the song, which did not exist previously[3]. Since the song is a 'new creation', it will be the intellectual property of the person who created it and not the singer, even though it was voiced that were used for the song. In a 2019 case, Jennifer Lopez was sued for copyright infringement over a photo of herself she uploaded on Instagram, with the photographer claiming that the shot was his intellectual property and that she did not obtain his permission before sharing it. Even though the photograph is of herself, the photograph is a creation of the mind of the photographer and hence, it is his intellectual property[4]. Hence, this case further reinforces the notion that it is the creator of the content who is the owner and not the person on whom the content is created.

Next, we have the question of whether there is an actual need for the regulation of deepfakes or not. To answer this one does not need to go far as we've all seen videos on social media platforms like Instagram and X, of PM Modi singing different songs which are made using AI, while these are harmless, one needs to understand the severity of how easy it is to replicate the voice or likeness of such a powerful person. There were reports wherein some voters got a call from US President Joe Biden asking them not to cast their votes in the elections[5]. There is also the issue of original content of artists being modified using AI and then being passed off as original and the original creators of the work not getting their fair share, which is ultimately a violation of their copyright. For instance, a song, titled 'Heart on My Sleeve', sounded like Drake and The Weeknd performing together, prompting it to get millions of clicks on streaming platforms and even getting submitted for Grammy consideration but it was ultimately discovered the song was a fake and the artists were not involved with it[6]. Universal Music Group, one of the largest music labels in the US raised concerns regarding the use of intellectual property in such cases stating, "*which side of history all stakeholders in the music ecosystem want to be on: the side of artists, fans and human creative expression, or on the side of deep*

[3] Ethan Shanfeld, 'Ghostwriter's Heart on my Sleeve, the AI generated song mimicking Drake and the Weeknd submitted for Grammys' (*Variety*, 6 September 2023) <https://variety.com/2023/music/news/ai-generated-drake-the-weeknd-song-submitted-for-grammys-1235714805/>

[4] Business Law and Litigation at Raymond Law Group LLC, 'Jennifer Lopez sued for copyright infringement' (*The National Law Review*, 7 May 2020) <https://natlawreview.com/article/jennifer-lopez-sued-copyright-infringement?amp>

[5] Ali Swenson and Will Weissert, 'New Hampshire investigating fake Biden robocall meant to discourage voters ahead of primary' (*AP News*, 23 January 2024) <https://apnews.com/article/new-hampshire-primary-biden-ai-deepfake-robocall-f3469ceb6dd613079092287994663db5>

[6] *Supra 3*

fakes, fraud and denying artists their due compensation[7].” Lastly, the use of deepfakes in explicit content cannot be ignored. Almost eighty percent of deepfake content is used to make explicit imagery and pornographic content. These images and videos are not only traumatic for the victims due to them being so realistic that it is next to impossible to tell if they are fake or real, but they are also being used as a means to extort or blackmail. The malicious use of deepfakes does not end here as they are also used for spreading misinformation, committing identity fraud, scams, etc. It is critical to enact laws to regulate AI because, while deepfake images and videos may be fake, their impact and repercussions can be very real. Hence, while not everyone who uses deepfake technology does so with malicious intent, those who do must bear the consequences of their actions.

However, regulation of deepfakes is easier said than done, due to the rapidly evolving technology and the use of Generative Adversarial Networks (GANs), which can continuously refine and improve the quality of their work the detection of deepfakes is becoming difficult with each passing day. The developers of deepfakes may easily include any software designed to detect fake videos into the GAN cycle, making the detection model obsolete[8]. One researcher developed detecting algorithms based on the fact that deepfakes do not blink like genuine humans. After releasing his article, the researcher received anonymous emails with deepfakes that passed his detection model's blinking test[9]. The difficulty is that regardless of what content-based approach researchers devise to detect deepfakes, creators will just incorporate their discoveries into their GANs, resulting in ever more powerful deepfakes. Professor Siwei Lyu from the University of Buffalo states that there are several approaches still under development but none of them are perfect yet[10].

---

[7] Joe Coscarelli, ‘An A.I. Hit of fake Drake and The Weeknd rattles the music world’ (*The New Tork Times*, 24 April 2023)
<https://www.nytimes.com/2023/04/19/arts/music/ai-drake-the-weeknd-fake.html>

[8] John Channing Ruff, ‘The Federal rules of evidence are prepared for deepfakes. Are you?’ (*The Review of Litigation, Vol 41. Iss. 1,* Winter 2021)
<https://www.proquest.com/openview/84ea49671c7f8712bb4b6cef482a6a51/1?pq-origsite=gscholar&cbl=37465>

[9] John P. LaMonaga, ‘A break from reality: Modernizing authentication standards for digital video evidence in the era of deepfakes’ (*American University Law Review, Vol. 69 Iss. 6*, August 2020)
<https://digitalcommons.wcl.american.edu/aulr/vol69/iss6/5/>

[10] Geoff Mulvihill, ’What to know about how lawmakers are addressing deepfakes like the ones that victimized Taylor Swift’ (*AP News*, 1 February 2024)
<https://apnews.com/article/deepfake-images-taylor-swift-state-legislation-bffbc274dd178ab054426ee7d691df7e>

Part 2: America's approach to deepfakes

America has always been the front-runner in the arena of IP rights, however, since the realm of AI is still in its infancy and different markets take different approaches, current legislation on deepfakes is somewhat fragmented. There is still no federal law that regulates or prohibits the creation or sharing of deepfake content, however, lawmakers are actively advocating for a change in the law to incorporate deepfakes either by amending the current copyright laws in force or bringing a new law altogether specifically designed to tackle this problem. The 'No Artificial Intelligence Fake Replicas and Unauthorized Duplications (No AI FRAUD) Act' was presented by legislators in January 2024. A federal framework to safeguard people against AI-generated fakes and forgeries is established by this law, which prohibits the unauthorized creation of digital depictions of anyone, alive or deceased and would apply to both their speech and look[11]. Additional suggested laws consist of: The 'Senate's Nurture Originals, Foster Art and Keep Entertainment Safe (No FAKES) Act', which would safeguard performers' voices and works of art and the 'Disrupt Explicit Forged Images and Non-Consensual Edits (DEFIANCE) Act' which would enable lawsuits pertaining to fake pornographic photographs and videos[12].

While there is no federal law as of now, some states have either already implemented it or are in the process of implementing their laws. California is at the forefront of AI regulations in the country and brought the first legislation regulating deepfakes back in 2019. This law not only criminalizes non-consensual use of deepfakes but also gives the victims the right to sue those who create images using their likenesses (Assembly Bill 602)[13]. Texas also introduced the 'Unlawful Production or Distribution of Certain Sexually Explicit Videos Act', making the production of explicit deepfake videos without the depicted person's permission a criminal offense. Apart from these states, the states of Hawaii, Florida, Illinois, New York and Minnesota have brought in their own laws. However, a common notion in these laws is that they focus primarily on the notion of explicit deepfake content and not so much on the intellectual property aspect of it, where there is still a need for strong regulation. According to Jake Morabito, director of communications and technology task force for the American

[11] Darin Klemchuk, 'The No AI FRAUD Act recognizes IP in all individuals. Plus, brand protection strategies' (*LinkedIn*, 8 March 2024) <https://www.linkedin.com/pulse/ai-fraud-act-recognizes-ip-all-individuals-plus-brand-darin-klemchuk-cqogc#:~:text=The%20No%20AI%20FRAUD%20bill,%2C%20abuse%2C%20fraud%2C%20etc>
[12] *Supra 1*
[13] *Supra 1*

Legislative Executive Council, "*lawmakers should not target the technology that can be used to create deepfakes, as that could shut down innovation with other uses*[14]."

Part 3: European Union's approach to deepfakes

The EU is one of the frontrunners when it comes to data protection and privacy, which is of paramount importance in this digital era. Hence, the EU proposed the Artificial Intelligence Act, the first of a kind, comprehensive AI law, back in April 2021, aimed at tackling the growing problem of data privacy in the ever-expanding and changing digital world. The legislation aims to make sure that AI systems used in the EU are safe, transparent, traceable, non-discriminatory and environmentally friendly[15]. The European Parliament adopted this Act on March 13, 2024. The Act does not bar the use of deepfakes but attempts to regulate them through obligations placed on creators, who are required to "*disclose that the content had been artificially generated or manipulated*[16]." While this new legislation might seem like the knight in shining armor, here to protect the victims of artificial manipulation of their image, it is not without its own share of flaws. The primary concern is enforceability, as it is still not clear how the law will apply to creators of malicious content who are operating from outside of the EU as the EU does not have jurisdiction beyond the boundaries of its member states. Furthermore, the question of whether the obligations of transparency will apply to creators who produce explicit deepfakes in their personal capacity instead of a professional one still persists.

The United Kingdom, which is no longer a part of the EU, despite heavy backlash passed a law called the 'UK Online Safety Act' in 2023, aimed at providing relief to those who have been distressed by the use of artificially manipulated images and videos[17]. While this Act does not prohibit the creation of explicit deepfakes or even criminalize the creation of any type of deepfake without the subject's consent, it sure takes a positive step in providing the affected party a mechanism for redressal whose IP has been used to create such false images and videos.

[14] *Supra 10*
[15] 'EU AI Act: First regulation on artificial intelligence' (*European Parliament*, 18 June 2024) <https://www.europarl.europa.eu/topics/en/article/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence>
[16] Emma Mifsud and Patrick Massa, 'Deepfakes and the law: Are we protected?' (*Lexology*, 28 August 2023) <https://www.lexology.com/library/detail.aspx?g=6de74674-e2d5-4e0c-9e26-33f4d6aadf40>
[17] Jon Porter, 'The UK's controversial Online Safety Bill finally becomes law' (*The Verge*, 26 October 2023) <https://www.theverge.com/2023/10/26/23922397/uk-online-safety-bill-law-passed-royal-assent-moderation-regulation>

Part 4: India's standing

At the moment India does not have any law that regulates or prohibits the creation or circulation of deepfakes. Sections 67 and 67A 'Information Technology Act' (IT Act) 2000 make the publishing and transmission of obscene material electronically a criminal offense[18], however, that limits the misuse of deepfakes to the domain of explicit content, while this is a major area where deepfakes are extensively used, it is not the only domain where such content can have grave consequences. For instance, in 2020, just before the Delhi elections a video of the BJP's Delhi President surfaced on the internet where he was seen criticizing his opponents, the video was eventually found to be a deepfake[19]. However, this incident raised concerns about such videos and images being used in the elections, which can have grave consequences for the country as a whole and the transmission of such content is outside the purview of the IT Act. Another significant area where deepfakes can cause a lot of damage is the financial sector as it can be used to gain unauthorized access to accounts or even manipulate markets. In a recent development, some fraudsters employed deepfake technology to impersonate the chief financial officer during a video conference, successfully deceiving an employee at an MNC into authorizing a $25 million payment[20]. This is just the tip of the iceberg as criminals can easily impersonate influential people like a company's top management and make statements harmful to the company's interests, influencing public sentiment and causing the share prices to fall[21]. Europol therefore considers deepfakes to be significant to 'perpetrating extortion and fraud, facilitating document fraud, falsifying online identities and fooling KYC mechanisms, falsifying or manipulating electronic evidence for criminal justice investigations, disrupting financial markets' and, for example, the theft of trade secrets[22].

Such use of deepfake content not only causes harm to the subject of the content but also tarnishes the image of the author of the content. Further in the *Amarnath Sehgal v Union of*

[18] Section 67 and 67A, Information Technology Act 2000
[19] Binayak Dasgupta, 'BJP's deepfake video trigger new worry over AI use in political campaigns' (*Hindustan Times*, 21 September 2020)
<https://www.hindustantimes.com/india-news/bjp-s-deepfake-videos-trigger-new-worry-over-ai-use-in-political-campaigns/story-6WPlFtMAOaepkwdybm8b1O.html>
[20] Heather Chen and Kathleen Magramo, 'Finance worker pays out $25 million after video call with deepfake chief financial officer' (*CNN World*, 4 February 2024)
<https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html>
[21] Bart van der Sloot and Yvette Wagensveld, 'Deepfakes: Regulatory challenges for the synthetic society' (*Computer Law & Security Review, Vol. 46*, September 2022)
<https://doi.org/10.1016/j.clsr.2022.105716>
[22] *Supra 21*

India case, the Delhi High Court recognized that an author also has moral rights over his work and also has the right to preserve, protect and nurture his creation and can claim damages if there is any distortion, mutilation or modification of his work in such a manner that tarnishes his reputation[23].

However, the question is how successful is the claim of copyright infringement against deepfakes? While copyright takedowns can be useful in taking down videos and images but one must remember that truly removing content can be a tedious task as evident from the recent episode where the morphed video of actress Rashmika Mandana was shared on X, even after claiming that the video was fake, the video is still in circulation and one can find it with just one Google search. The burden of proof also lies on the copyright owner to prove that the hyper-realistic deepfake is an infringement of his protected work and proving this can be a tedious task due to the problems discussed earlier. Furthermore, the more harrowing loophole in the use of copyright for the regulation of deepfakes is that the copyright may not be with the subject of the fake content, for instance in the Jennifer Lopez case the copyright was with the photographer and not the actress, making it extremely difficult for her to get the content removed if her photograph was used for a deepfake as she is not the holder of the copyright over it. Hence, copyright claims can be seen as only a temporary solution for the issues of consent and ownership of our own likenesses online[24] (Nema, 2021).

Apart from this the use of deepfakes also infringes the privacy rights of individuals, as recognized in the *KS Puttaswamy* case[25], as their fake videos are made without their consent. The interference in privacy is acceptable only when it falls under the domain of fair use as per Section 52 of the IT Act but if the deepfake is used for fair use then due recognition to the author and the copyright owner of the original content has to be given as provided by the Act[26]. Another positive step taken towards the regulation of deepfakes is the recognition of the right to be forgotten, as under this provision any circulation of personal data in the public domain, that stems from unauthorized use of the said data, can be stopped and erased altogether by order of the Court. This is particularly useful in cases of revenge porn as it will help the victims to

[23] Amarnath Sehgal v Union of India 117(2005) DLT717
[24] Purvi Nema, 'Understanding copyright issues entailing deepfakes in India' (*International Journal of Law and Information Technology, Vol. 29 Iss. 3*, *October 2021)*
<10.1093/ijlit/eaab007>
[25] Justice K.S. Puttaswamy (Retd.) v Union of India and Ors (2017) 10 SCC 1
[26] Section 52, Information Technology Act 2000

get the fake content removed from the public domain.

Part 5: The unique problem of India and AI

Union IT Minister Ashwini Vaishnaw has termed deepfake technology as a '*threat to democracy*' as it threatens the very fabric of society by blurring the lines between what is real and what is fake[27]. Plus, with the advent of Jio, India's telecom market was revolutionized as a lot of people not only got access to fast, uninterrupted internet connection but also got their hands on a smartphone for the first time. Internet penetration in India increased from a mere 13.5% in 2014 to 52.4% in 2024 with an 8% year-on-year growth and is projected to reach 66% by 2027[28]. However, as a result of low-cost internet, rising average incomes and the flood of Chinese smartphones that provide great value for a low price, a large portion of this population is gaining access to the internet and smartphones for the first time and is thus not tech-literate. According to statistics, the number of smartphone users in India increased from 191.6 million in 2014 to over a billion in 2023, with an additional fifty million projected by 2040, making them perfect targets for deepfake fraud owing to their lack of knowledge of the digital world[29]. Furthermore, unlike other major countries, India still does not have well-defined legislation to tackle the current AI problems as the IT Ministry's promise to implement rules to curb the menace of deepfakes by the first week of December 2023 is yet to be fulfilled[30]. We still rely on the IT Act 2000, which has become obsolete as it does not even recognize deepfakes. Furthermore, while Rule 4(2) of the 2021 IT Guidelines mandates social media sites to identify originators of information, platforms like Meta and Twitter contest these rules and have filed a plea in the Delhi High Court, citing it as a breach of user privacy and a threat to end-to-end encryption[31].

---

[27] PTI, 'New regulation to tackle deepfakes soon, says IT minister Ashwini Vaishnaw' (*National Herald*, 23 November 2023)
<https://www.nationalheraldindia.com/science-tech/new-regulation-to-tackle-deepfakes-soon-says-it-minister-ashwini-vaishnav>

[28] Tanushree Basuroy, 'Internet penetration rate in India from 2014 to 2024' (*Statita*, 15 May 2024)
<https://www.statista.com/statistics/792074/india-internet-penetration-rate/>

[29] Shangliao Sun, 'Number of smartphones users in India in 2010 to 2023, with estimates until 2040' (*Statista*, 18 September 2023)
<https://www.statista.com/statistics/467163/forecast-of-smartphone-users-in-india/>

[30] Shivani Shinde, 'India to have draft regulation on deepfakes in 10 days: Ashwini Vaisnaw' (*Business Standard*, 23 November 2023)
<https://www.business-standard.com/india-news/india-to-have-draft-regulation-on-deepfakes-in-10-days-ashwini-vaisnaw-123112300437_1.html>

[31] Nandini Singh, 'Why is WhatsApp threatening to leave India? Everything you need to know' (*Business Standard*, 26 April 2024)

The absence of robust legislation to regulate and govern the use of AI, coupled with the deep penetration of the Internet among a largely tech-illiterate population, renders India's interaction with deepfakes unique and positions it as a hotspot for AI-related crimes.

Part 6: What can be done?

The most evident and primary course of action to address this issue is the introduction of specialized legislation to regulate AI, akin to the EU's AI Act. Additionally, there is a pressing need to raise awareness about the misuse of AI through public information campaigns, particularly targeting Tier 2 and Tier 3 cities, towns, and villages so that people can critically evaluate digital content and identify deepfakes. These campaigns can be made more effective by targeting specific segments of society that are particularly vulnerable to such attacks or frauds and may require specialized and immediate attention. For instance, over 86% of senior citizens are unfamiliar with digital technology, making them more susceptible to fraud[32]. Additionally, due to the generational gap, they may need extra assistance in learning how to use this technology. Furthermore, companies should be encouraged to implement self-regulation of AI usage on their platforms, such as incorporating labeling features to identify artificially generated content. For example, Google recently introduced a generative AI feature for editing photos on Android 15, yet imposed restrictions on its use concerning human body parts and Samsung explicitly marks the photos with a 'Made with AI' tag that has been generated using their AI. Similarly, Meta and Microsoft have established dedicated teams, known as Oversight Boards, responsible for reviewing content on their platforms and removing any material deemed harmful to public interests.

Lastly, on the constitutional level, there is a need to develop the 'Right to Personality' as a separate constitutional right. Currently, the right has mostly been considered in relation to influential persons and celebrities, whose likenesses are frequently utilized for illicit economic benefit, although this also limits the right. While the Indian Copyright Act 1957 does not explicitly distinguish between public and non-public figures, courts have frequently interpreted the law in a way that creates this distinction, making it difficult for a common citizen to use

<https://www.business-standard.com/india-news/why-is-whatsapp-threatening-to-leave-india-everything-you-need-to-know-124042600417_1.html>

[32] Anand Singh and Sujay B M, 'Tangled web: Senior citizens navigate a complex digital world' (*Deccan Herald*, 7 April 2024) <https://www.deccanherald.com/india/karnataka/bengaluru/tangled-web-senior-citizens-navigate-a-complex-digital-world-2968208>

this right to protect their identity. "*The broader interpretation of this right is the first step to the idea that a person may automatically have an inherent right to control the usage of their identity*[33]." Interpreting the Right to Personality in a way that respects individual dignity and privacy is necessary. In order to ensure that the whole population, not just celebrities, is safeguarded, it should also guard against non-commercial abuses like revenge porn and market manipulation in addition to the commercial use of someone's identity[34].

Conclusion:

The Delhi High Court's recent ruling in the *Anil Kapoor v. Simply Life India*[35] case safeguarding actor Anil Kapoor's name, image, and voice against unauthorized use—like in deepfakes—is encouraging and indicates that India is making progress in regulating AI-generated content[36]. Although this judgment represents a positive step forward, it fails to provide clear protection for the general public, as Anil Kapoor was granted protection primarily due to his status as a well-known public figure. The Right to Personality still does not extend its protections to the broader population. Hence, more needs to be done to address the Indian legal system's lack of a regulatory framework to address the issues of the digital age.

Since there has not been any foolproof technological solution to tackle the threat of unregulated deepfake content, we need to turn to the realm of legislation to try and find a solution. While there is no permanent solution to the issue of deepfakes anywhere in the world, India can have the second mover advantage by learning and borrowing from the legislations of other countries and then molding it according to her own needs. However, prohibiting the use of generative is not a viable option as that may cripple innovation, instead, we can make regulations that prompt companies like OpenAI, whose platforms are used to generate such realistic content implement better systems to prevent malicious deepfakes from being created and there should be legal consequences those who do it anyway. Furthermore, active steps should be taken to encourage companies to self-regulate content that is generated using their platform or shared on their

[33] Khushi Saraf and Akshay Sriram, 'The Dilemma of Deepfakes: Expanding the ambit of Right to Personality to regulate deepfakes in India' (*Law School Policy Review*, 4 May 2024) <https://lawschoolpolicyreview.com/2024/05/04/the-dilemma-of-deepfakes-expanding-the-ambit-of-right-to-personality-to-regulate-deepfakes-in-india/>

[34] *Supra 33*

[35] Anil Kapoor vs. Simply Life India and Ors. (2023) MANU/DEOR/248558/2023.

[36] Nupur Thapliyal, 'Delhi High Court protects actor Anil Kapoor's personality rights, restrains use of his name, image or voice without consent' (*Live Law*, 20 September 2023) <https://www.livelaw.in/top-stories/delhi-high-court-anil-kapoor-voice-image-misuse-personality-rights-238217>

platform. This self-regulation can be attributed to the company's corporate responsibility towards society. India can also learn from the UK's model and build a robust redressal system for those who have been affected by either the infringement of their work due to deepfakes or due to their likenesses being used in such content.

In conclusion, the field of AI is rapidly advancing and with the emergence of generative AI integrated into consumer operating systems like Apple Intelligence and Adobe Photoshop, it has become exceedingly simple for individuals with even basic knowledge of command prompts and audio-video editing to create hyper-realistic deepfakes. The Indian Government needs to change its perception of deepfake technology being limited to fake news[37], as it has proved to have grave and real consequences. However, even when created just for entertainment, deepfakes can potentially infringe the copyright and right to privacy of an individual, hence this issue needs to be given proper attention when it is still in its infancy instead of waiting for it to become an out-of-control problem.

[37] Government of India, Ministry of Electronics and Information Technology, Lok Sabha Unstarred Question, Deepfake Technology, (4 December 2019)