Educational Administration: Theory and Practice
2024, 30(1), 7751-7760
ISSN: 2148-2403
https://kuey.net/

Research Article

Legal Challenges and Advantages of Deep Fake in Indian Regulations

Abhishek Singh[1*]

[1*]Central Government Standing Counsel **Department** Armed Force Tribuanl, RB Jaipur Apex University Jaipur Mail Id abhisheksingh9772201345@gmail.com

Citation: Abhishek Singh (2024). Legal Challenges and Advantages of Deep Fake in Indian Regulations., *Educational Administration: Theory and Practice*, 30(1) 7751-7760
Doi: 10.53555/kuey.v30i1.10917

ARTICLE INFO

ABSTRACT

Deepfakes are a rapidly expanding high-tech trend that is changing a variety of digital pathways, encompassing internet access and media production. They provide a range of benefits to both authors and users. They can offer entertainment value, for instance, by enabling users to make sarcastic or hilarious adaptations of pre-existing media content without needing to shoot brand-new sequences. By producing cinematic extras or background characters, they may also automate the creative process. Deepfakes may also be employed in medical applications, such as virtual assistants for physicians who need help while consulting with patients who live distant from clinics or hospitals. Deepfakes are dangerous to society, though, because they may be used maliciously to disseminate misleading information or profit on the likenesses of others. Different kinds of rules have been enacted in jurisdictions all around the world to solve these issues. These regulations forbid the use of manipulated audio and video recordings in an effort to sway election results. In an effort to alert viewers that what they are viewing might not necessarily be accurate depictions of events, several nations have even gone so far as to mandate that businesses creating deepfake content label themselves as such. The definition of deepfakes, their possible advantages and disadvantages, the many kinds of deepfakes that are out there, and India's attempts to control them will all be covered in this essay. In order to reduce the dangers of deepfakes while maintaining their creative potential, the author will also provide some policy proposals.

KEYWORDS: Indian Regulations, advantages of deepfakes, legal challenges, danger, deepfakes
SUBJECTS: Artificial Intelligence (AI); Cognitive Artificial Intelligence; Cybercrime

1. Introduction

False news has recently become a challenge to democratic governments, public communication, and human civilization. Fake news is false information invented to mislead people. Untrue stories are disseminated rapidly via social media, where they can affect numerous users. Currently, one out of five users of social media obtains an information through YouTube and Facebook (Westerlund, 2019)[1]. As video has become more popular, it is now necessary to verify whether news and media messages are authentic, as new technological equipment and facilities make videos appear convincing. Social media platforms make it simple to collect and disseminate false information, making it more challenging to determine what is reliable and leading to risky judgments. Truly, the world where we exist at present is what is referred to as 'post-truth' era by some people, which is defined by online misinformation and information conflict controlled by malicious players who run free content campaigns to control public views (ibid). With the latest progress in technology, creating what is now referred to as 'deepfakes', hyper-realistic films are easy to create by swapping faces that show no or little sign of being manipulated. Deepfakes, which are powered by latest advancements in AI as well as machine learning

[1] Westerlund, M. (2019). The emergence of Deepfake technology: A review. Technology Innovation Management Review, 9(11), 39–52. https://doi.org/10.22215/timreview/ 1282

(ML), enable automated systems to produce counterfeit content that is more sophisticated and challenging to detect (Kietzmann et al., 2020)[2]. For example, deepfake technology may produce official, humorous, or sexual recordings of individuals saying anything without the consent of the people whose voices and images have been used. The scale, scope, and intricacy of the technology used in deepfakes are the most noteworthy features, since nearly anybody with a computer can produce fake films that are indistinguishable from real ones. Deepfakes will probably be employed more often in the coming years for revenge pornography, victimization, fabricated video proof in court, political harm, radical propaganda, threats, market control, and false news, in contrast to early forms that focused on employing the faces of politicians, artists, clowns, and performers in pornographic films (2020). While spreading fake news is simple, stopping deepfakes is really challenging. Understanding deep fakes, their causes, and the software that creates them is necessary to counteract them. However, scholarly research on online disinformation in social networks has just recently begun. As a development of generative networks in adversarial training, deepfake technology trains an AI system by concurrently optimizing two neural networks: one that creates data and another that analyzes data to determine its correctness. Generative adversarial networks (GANs) are employed in deepfake technology to alter photos or videos to create realistic-looking fakes that are hard to tell apart from genuine ones. While discriminator network learns to differentiate between authentic and fraudulent material, the generator network produces the bogus content. This process is repeated until the generator produces content that is almost identical to real content, resulting in a convincing deepfake. The use of GANs in deepfake technology enables bad actors to create sophisticated fakes on a large scale, presenting significant challenges to integrity of data and democratic processes. As deepfake technology continues to evolve, researchers recognize the need to develop defences against it. One approach is to use the same AI technologies that generate deepfakes to detect them, creating anti-deepfake algorithms that can identify subtle differences between real and fake content. Creating government regulations to encourage openness, responsibility, and moral application of deepfake technology is one additional strategy. In general, as deepfake technology advances, it is more critical than ever to develop practical measures to stop its malevolent utilization and inform public about its possible dangers and abuse. Therefore, this work aims to define deepfakes, find out who created them, study their importance, the harmful effects of their technology, give some examples of recent deepfakes, and explain how to fight against them. In this context, this work examines many news reports on deepfakes obtained from the websites of news media. By providing a thorough analysis of deepfakes and establishing the developing subject in a scholarly framework that acknowledges other options for combating deepfakes, this work contributes to the expanding body of research on false news and deepfakes (2020). Through a review of the existing literature, this paper demonstrates the challenges of deepfakes in the Indian context. The meaning of deepfakes has been given in 2nd section. Then article explains deepfake problem in section three. The benefits of deepfake technology are described in section four. Types of deepfakes are explained in section five. The 'Regulating Deepfakes: The Indian Perspective' section describes the regulation of deepfakes in India. Finally, sections seven and eight will propose some solutions and recommendations to tackle deepfake technology offenses.
Contribution of the study

2.1 Legal complexities and regulatory framework

By employing deepfake as a framework to analyze the current legal structure and frameworks that help address the difficulties posed by this technology, including privacy law, intellectual property rights, defamation law, cybersecurity issues, and others that have been identified as significant concerns, the present research contributes insights into the legal complexities surrounding deepfake technology in India. This thorough research clarifies the legal landscape around this matter and highlights the necessity of a strict regulatory framework to handle the complex effects of deepfakes.

Ethical and societal implications

The research touches upon ethical and societal aspects of deepfake technology and its possible aftermath attributable to instilling the customers in privacy violations, gender discrimination, violence, and political subversiveness. In doing so, the present study engages with some major issues in the wider discussion related to the ethical concerns and societal implications of the proliferation of false narrative-shaping tools such as deepfakes. It highlights the necessity of principles and sensitivity toward the bad impacts of deepfake technology.

Policy recommendations and legislative actions

Using policy action and legislative steps, the study formulates suggestions for the problems posed by deepfakes. Suggesting proactive adoption to the rapidly evolving technological scene, the study asserts the importance of policy action, which ensures persistent innovative momentum while keeping the risks that deepfakes present

[2] Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat? Business Horizons, 63(2), 135–146. https://doi.org/10.1016/j.bushor.2019.11. 006

at hand. This contributes to designing the guiding tools for policymakers and their regulating actors based on developing appropriate mechanism for deepfake technology.

Awareness and education

Another important factor in lowering the unlawful use of deepfakes is public awareness. The research focuses on the significance of ongoing education for people, companies, and regulatory authorities; developing cyber resilience and digital literacy; and building a better, safer society. This emphasis on education and awareness is a preventative tactic that gives people the tools to evaluate digital content and lessen the impact of deepfakes.

2. What are deepfakes?

Combining the words "deep learning" and "fake," "deepfakes" describes technique of editing incredibly realistic digital film to depict people talking and acting in ways that never occurred (CNN, 2022)[3]. Neural networks that examine enormous volumes of data samples are used by deepfakes to learn how to imitate a person's voice, facial expressions, behavior, and inflections. Two people's videos must be input into a deep learning system in order to teach it to replace faces. This indicates that deepfakes use an AI technique that modifies or swaps out a person's face in a video for another person's (CNN, 2022; Dickson, 2022)[4]. In 2017, an anonymous Reddit user dubbed themselves "Deepfakes," coining the phrase "deepfake." One Reddit user created and shared modified pornographic videos by manipulating Google's open-source, deep-learning technology. Face-swapping is a method employed to alter the videos. The user "Deepfakes" substituted famous faces for real ones. Although the use of deepfakes in marketing might be deleterious to the average consumer who may be influenced under the premise of misleading influencer marketing, the capacity to edit footage of prominent people has additional potentially catastrophic implications, especially with regard to political significance (Mostert & Perot, 2020)[5]. Because deepfakes use genuine film, can contain real audio sound, and are upgraded for quick distribution on social media, they are difficult to spot (Westerlund, 2019)[6]. Because of this, a lot of individuals believe that what they are seeing is genuine. Due to consumers' propensity to follow the herd, deepfakes target social media sites where falsehoods, gossip, and conspiracies spread swiftly. Furthermore, a persistent "infopocalypse" leads people to feel that they can't believe anything unless it originates from their social media accounts and is backed up by their loved ones, close friends, and preconceived notions. Indeed, many people accept anything that confirms their pre-existing opinions, even if they doubt its authenticity. Low-priced fakes, which are low-quality videos with slightly manipulated genuine information, are prevalent due to the wide availability of cheap hardware, such as effective graphical processing units. Excellent, precise deepfakes for disinformation may be made with free software. This makes it possible for people with limited technical skills and no artistic understanding to virtually perfectly edit movies, swap out faces, adjust gestures, and create speeches [ibid].

3. Deepfakes problem

By using "deepfake" technology, real people might appear to be saying and doing things that never actually happened. Deepfakes are commonly utilized to entertain people, including DeepTomCruise (funny videos that look like Tom Cruise) or the ReFace app, which enables a person to put their face on a superstar music video or film clip quickly (Laser, 2022)[7]. Additionally, deepfake technology is employed in a negative manner. For instance, between 90 and 95 percent of deepfakes on the internet are nonconsenting porn, which entails putting a victim's face on pornographic content and may be emotionally and character-damaging [ibid]. The platform has been used to produce non-consensual false pornography and sexual images, but there is a chance

---

[3] CNN. (2022). The Fight to Stay Ahead of Deepfake Videos before the 2020U.S. Election. Retrieved November 27, 2022, from https://edition.cnn.comdeepfake -2020-detection/index.html

[4] CNN. (2022). The Fight to Stay Ahead of Deepfake Videos before the 2020U.S. Election. Retrieved November 27, 2022, from https://edition.cnn.comdeepfake -2020-detection/index.html, Dickson, B. (2022). Blurs the line between reality and fic tion. Retrieved from https://www.pcmag.com/news/ when-ai-blurs-the-line-between-reality-and-fiction

[5] Mostert, F., & Perot, E. (2020). Fake it till you make it: an examination of the US and English approaches to per sona protection as applied to deepfakes on social media. Journal of Intellectual Property Law & Practice, 15(1), 32–39. https://doi.org/10.1093/jiplp/jpz164

[6] Westerlund, M. (2019). The emergence of Deepfake technology: A review. Technology Innovation Management Review, 9(11), 39–52. https://doi.org/10.22215/timreview/ 1282

[7] Laser, C. D. (2022, November 27). Privacy & freedom of speech. Retrieved from https://yourwitness.csulaw.org/ uncategorized/deepfakes-privacy-and-freedom-of speech/.

[8] Gosse, C., & Burkell, J. (2020). Politics and porn: How news media characterizes problems presented by deepfakes. *Critical Studies in Media Communication, 37*(5), 497–511.

that it may soon be used for politically inappropriate purposes (Gosse & Burkell, 2020)[8]. Deepfakes are capable of transforming existing audiovisual and artificially made content to provide the impression that they conform to a certain class of actual realities (Gregory, 2019)[9]. According to journalism, deepfakes are a risky technique that might skew people's understanding of sociopolitical realities (Yadlin-Segal & Oppenheim, 2021)[10]. Psychological safety is also threatened by the proliferation of deepfakes, which also perpetuate gender differences in visual information (Afanasyeva & Yumasheva, 2022; Wagner & Blewer, 2019)[11] (Pantserev, 2020)[12]. Deepfakes also threaten business and state safety and are utilized by players abroad in social impact campaigns. They can also be utilized to impersonate companies' staff for financial crime, according to a Private Industry Notification by the F.B.I. in March 2021 [2020]. Furthermore, the issue of deepfake technology has drawn more attention in recent years. People's lives and reputations can be harmed by the widespread dissemination of false information made possible by this technology. Along with impersonating famous personalities, it may also be used to produce sex movies and false news. Deepfake technology is continuously evolving and getting more sophisticated, endangering the integrity of democratic institutions and political processes. In order to detect deepfakes and stop them from being exploited to sway public opinion, policymakers and tech corporations need to collaborate. Addressing this issue is crucial to preserving information integrity and stopping the dissemination of inaccurate and deceptive content.

4. The benefits of deepfake technology

Although it has made it much harder to distinguish fact from fiction, this has created exciting new opportunities in a variety of industries, including video games, visual arts, business, and movies (Verdoliva, 2020)[13]. Movie theaters, academic media, virtual interactions, games, shows, material science, healthcare, social media, and other economic sectors like fashion and e-commerce are just a few of the industries that benefit from the Deepfake program (Taulli, 2022)[14]. In addition to becoming common, the combination of photography and cutting-edge technology also significantly changes medical practice (Crystal et al., 2020)[15]. For example, a solution leveraging deepfake capability might safeguard privacy in medical videos (Zhu, 2020)[16]. Deepfake technology can be beneficial to the movie industry in many areas and aspects. For instance, it can produce virtual voices for actors whose voices are damaged by diseases; it can also update the footage of the movie instead of reshooting the entire movie (Dickson, 2022)[17]. Film producers can reproduce standard parts in films, produce novel films featuring actors that died long ago, utilize special effects and high-quality face editing in post-production, and enhance substandard videos to high quality (Kan, 2022; Laser, 2022)[18].

---

[9] Gregory, S. (2019). Cameras everywhere revisited: How digital technologies and social media aid and inhibit human rights documentation and advocacy. Journal of Human Rights Practice, 11(2), 373–392. https://doi.org/10. 1093/jhuman/huz022

[10] Yadlin-Segal, A., & Oppenheim, Y. (2021). Whose dystopia is it anyway? Deepfakes and social media regulation. Convergence, 27(1), 36–51. https://doi.org/10.1177/ 1354856520923963

[11] Afanasyeva, T., & Yumasheva, I. (2022). Research on the effects of "DeepFake" Technology for the modern digital space. In Challenges and solutions in the digital economy and finance (pp. 57–65). Wagner, T. L., & Blewer, A. (2019). "The word real is no longer real": Deepfakes, gender, and the challenges of AI altered Video. Open Information Science, 3(1), 32–46. https://doi.org/10.1515/opis-2019-0003

[12] Pantserev, K. A. (2020). The malicious use of AI-based deepfake technology as a new threat to psychological security and political stability. In Cyber defence in the age of AI, smart societies and augmented humanity (pp. 37–55).

[13] Verdoliva, L. (2020). Media Forensics and DeepFakes: An overview. IEEE Journal of Selected Topics in Signal Processing, 14(5), 910–932. https://doi.org/10.1109/JSTSP. 2020.3002101

[14] Taulli, T. Deepfake: What you need to Know, Forbes. (2022, November 28). Retrieved November 27, 2022, from https://www.forbes.com/sites/tomtaulli/2019/06/15/ deepfake-what-you-need-to-know/?sh=1298d58d704d.

[15] Crystal, D. T., Cuccolo, N. G., Ibrahim, A. M. S., Furnas, H., & Lin, S. J. (2020). Photographic and video deepfakes have arrived: how machine learning may influence plastic surgery. Plastic and Reconstructive Surgery, 145(4), 1079- 1086. https://doi.org/10.1097/PRS.0000000000006697 de Seta, G. (2021).

[16] Zhu, B., Hao Fang, Yanan Sui, and Luming Li. (2020). Deepfakes for medical video de-identification: Privacy protection and diagnostic information preservation. In Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, ACM, pp. 414–20

[17] Dickson, B. (2022). Blurs the line between reality and fiction. Retrieved from https://www.pcmag.com/news/ when-ai-blurs-the-line-between-reality-and-fiction

[18] Laser, C. D. (2022, November 27). Privacy & freedom of speech. Retrieved from https://yourwitness.csulaw.org/ uncategorized/deepfakes-privacy-and-freedom-of speech/. Laskovtsov, A. (2020). Navigating the manosphere: An examination of the Incel movements' attitudes of sexual aggression and violence against women.

Deepfake software can assist in automatically and realistically dubbing voices for movies in any language, enabling a variety of audiences to experience academic and cinematic works. David Beckham broke down barriers to communication in a 2019 worldwide malaria awareness campaign by using voice-changing and visual technologies in a bilingual advertisement. Additionally, the deepfake program can break down the barriers to communication on video seminar calls by converting utterances and changing facial and mouth expressions to enhance eye contact and make everybody seem to be using a similar language (Dickson, 2022)[19]. Deepfakes' mechanism enables synthetic duplicates of individuals, high telepresence online chat environments, multiplayer games, and smart assistants that appear and sound natural (PCM09). This creates good relations among people and communication on the internet. Technology can also be positively used in the medical and social fields. Deepfakes can assist individuals in coping with loss of their loved ones by virtually bringing the dead person alive again, allowing their grieving friends/relatives to bid them goodbye. In addition, it can digitally reproduce a limb that was amputated or help transgender individuals express their gender. It can make Alzheimer's patients relate to a younger face they can recall (FOX05). Researchers are investigating how to utilize GANs to identify defects in X-rays and their potential to create actual chemical molecules to accelerate material science and medical findings (Westerlund, 2019)[20] Companies, like brands, can apply deepfake technology, for it can change e-commerce and advertising outstandingly. For instance, brands can employ people as highly fashionable models, but in reality, they are not, and display fashionable clothes on different models with diverse skin tones, weights, and heights. Deepfakes can turn customers into models via super-personalized content; the technology allows actual fitting to see beforehand how they would look in clothing before buying it, and can produce targeted clothing style adverts that differ based on weather, viewer, and time. In addition to allowing people to digitally clone themselves and carry these personal avatars with them across online retailers, the technology can let consumers try on wedding dresses and suits quickly and electronically, as well as experience a wedding scenario. Additionally, AI may produce unique phony voices that help brands and products stand out (Westerlund, 2019)[21]. Furthermore, deepfakes can be utilized to produce videos where the management of a corporation is harmed or engages in unpleasant behavior to forcefully reduce the amount of stock. Deepfakes can also be partly used as spear-phishing attacks (efforts to manipulate a targeted receiver to distribute clandestine content or send cash to a malevolent player). Deepfakes may also be employed to cause harm by falsely portraying armed cops or politicians engaging in violent conduct. Moreover, as deepfakes gain more popularity, they make malicious players hold that real pictures are false, which Professors Chesney and Citron refer to as 'the liar's share' (Afanasyeva & Yumasheva, 2022; Wagner & Blewer, 2019)[22]. Smoothly replacing one person's face in video with another is getting simpler and easier with a pre-trained generative adversarial network (GAN) (Korshunov, n.d.)[23]. Each of these uses has the potential to significantly affect modern culture, interpersonal relationships, political systems, and foundations of law and order (vander Sloot & Wagensveld, 2022)[24]. According to Mosert and Perot (2020)[25], the widespread occurrence of "deepfakes" in particular calls into doubt the applicability of current laws and presents fresh difficulties for established regulations. Deepfakes have the potential to perpetuate the internalization of rape, support for violence against women, victimization and repression, sexual privilege, and gender issues (Laskovtsov, 2020)[26], since perpetrators of domestic violence may utilize them to extort, threaten, and assault victims (Lucas, 2022)[27].

---

[19] Dickson, B. (2022). Blurs the line between reality and fiction. Retrieved from https://www.pcmag.com/news/ when-ai-blurs-the-line-between-reality-and-fiction

[20] Westerlund, M. (2019). The emergence of Deepfake technology: A review. Technology Innovation Management Review, 9(11), 39–52. https://doi.org/10.22215/timreview/ 1282

[21] Westerlund, M. (2019). The emergence of Deepfake technology: A review. Technology Innovation Management Review, 9(11), 39–52. https://doi.org/10.22215/timreview/ 1282

[22] Afanasyeva, T., & Yumasheva, I. (2022). Research on the effects of "DeepFake" Technology for the modern digital space. In Challenges and solutions in the digital economy and finance (pp. 57–65), Wagner, T. L., & Blewer, A. (2019). "The word real is no longer real": Deepfakes, gender, and the challenges of AI altered Video. Open Information Science, 3(1), 32–46. https://doi.org/10.1515/opis-2019-0003

[23] Korshunov, P. n.d. Vulnerability assessment and detection of Deepfake videos. In Marcel, S., 2019 International Conference on Biometrics (ICB). Crete, Greece: IEEE, pp. 1–6.

[24] vander Sloot, B., & Wagensveld, Y. (2022). Deepfakes: regulatory challenges for the synthetic society. Computer Law & Security Review, 46, 105716. https://doi. org/10.1016/j.clsr.2022.105716

[25] Mostert, F., & Perot, E. (2020). Fake it till you make it: an examination of the US and English approaches to per sona protection as applied to deepfakes on social media. Journal of Intellectual Property Law & Practice, 15(1), 32–39. https://doi.org/10.1093/jiplp/jpz164

[26] Laskovtsov, A. (2020). Navigating the manosphere: An examination of the Incel movements' attitudes of sexual aggression and violence against women.

[27] Lucas, K. T. (2022). Deepfakes and domestic violence: Perpetrating intimate partner abuse using video technology. Victims & Offenders, 17(5), 647–659. https://doi. org/10.1080/15564886.2022.2036656 Maas

5. Types of deepfakes

We have four main kinds of deepfake creators:
(1) The public of deepfake hobbyists,
(2) Governmental actors like politicians abroad and different promoters,
(3) Other malicious players, like swindlers, and
(4) Real players like television establishments.

It is hard to detect people in deepfake hobby societies. In late 2017, after a user introduced celebrity porn deepfakes into Reddit, the recently created deepfake hobbyist community gained 90,000 members within a few months (Patterson, 2022)[28]. Many hobbyists concentrate on deepfakes related to pornography, while others place popular stars in movies in which they were never involved to create humorous impacts. Because they view AI-generated films as a creative solution to a puzzle rather than a means of deceiving or threatening others, hobbyists frequently view them as a new kind of virtual humor and support advancement of this technology. Their deepfakes can help them attract followers on social media and are mostly amusing, entertaining, or used to parody governments. Some hobbyists seek tangible gains for themselves, such as making people aware of the uses and benefits of deepfake technology to obtain a paid job related to deepfakes, for instance, with television programs or music videos. Therefore, hobbyists and real players like television enterprises can work together (ibid). Although hobbyists' meme-like deepfakes can provide virtual entertainment, there are also more malicious individuals at play. Many government agencies, political activists, hacktivists, radicals, and foreign countries can employ deepfakes in their misinformation efforts to influence public opinion and undermine trust in a nation's institutions. During these periods of hybrid warfare, deepfakes are instruments used to propagate misinformation, interfere with elections, and spark civil unrest. We can expect many internal and external 'troll farms' sponsored by states online that apply AI to produce and distribute false political videos designed to exploit internet users' particular prejudices. Deepfakes are highly used by scammers to manipulate markets and stocks, as well as for other economic fraud. Fraudsters use false videos produced by AI to mimic a manager via phone, demanding a quick transfer of money. Video calls can also be falsified in real-time in the future. Graphical tools needed to impersonate managers can be found online. Deepfake technology can impersonate managers visually and via audio; TED Talk videos on YouTube are an example (ibid). The identification conundrum is assessed by a diverse group of stakeholders, including experts from academia, technological platforms, media organizations, and civil society groups (Leibowicz et al., 2021)[29]. Numerous deepfakes on social media nowadays, such as Facebook or YouTube, can be perceived as inoffensive humor or creative works where living or dead celebrities are used. However, deepfakes also have negative implications, including personality along with revenge pornography, moreover efforts to manipulate politically and non-politically. Many deepfakes concentrate on public figures, political elites, and business executives because their real photos and videos flood the internet, which is used to develop the extensive image stockpiles required for training AI deepfake systems (Westerlund, 2019)[30]. Many of these deepfakes include errors, tricks, and humorous memes. For example, a deepfake may depict Nicolas Cage in movies he was not actually involved in, such as 'Terminator 2' or 'Indiana Jones'. A video of Bill Hader on "Late Night with David Letterman" and a movie that replaces Alden Ehrenreich with a teenage Harrison Ford in snippets taken from "Solo: A Star Wars Story" are two intriguing examples of deepfakes. Hader's visage changes to that of Tom Cruise when he speaks about him. Some deepfakes even feature the faces of deceased popular people, such as Rami Malek, the former vocalist of Queen, performing Beyonce's "Halo" with Freddie Mercury's visage superimposed on his face (ibid). There have been various applications of deepfake technology, such as a MAP (Museum of Art and Photography). In partnership with Accenture Labs, they have unveiled M. F. Husain's first conversational digital persona in India. One of India's most captivating artists, Husain's persona offers a look into his life and work through a unique digital experience designed to attract audiences of all ages. Another AI tool creates videos that depict the target as a skilled dancer by superimposing an actual dancer's motions onto their body, making them dance like a leading female ballet dancer. Dangerous deepfakes are increasing daily. The deepfake method allows for the creation of public figures and revenge pornography,

[28] Patterson, D. (2022). From deep fake to cheap fake, it's getting harder to tell what's true on your favorite apps and Websites, [C.B.S. News]. Retrieved November 30, 2022, from https://www.cbsnews.com/.

[29] Leibowicz, C. R., McGregor, S., & Ovadya, A. (2021). The Deepfake Detection Dilemma: A multistakeholder exploration of adversarial dynamics in synthetic media. In AIES'21: Proceedings of the 2021 AAAI/ACM Conference on AI, Ethics, and Society, July 2021, pp. 736–744.

[30] Westerlund, M. (2019). The emergence of Deepfake technology: A review. Technology Innovation Management Review, 9(11), 39–52. https://doi.org/10.22215/timreview/ 1282

which involves using images of public and non-public figures in pornographic content on social platforms without their consent. As a result of their faces being placed over faces of pornographic actors, celebrities encompassing Scarlett Johansson have been misrepresented in adult films (ibid). Deepfakes have been employed in politics for a number of reasons.

A video of a serving minister urging voters to vote against the current state administration was distributed to hundreds of thousands of electors in Telangana, which is set to hold elections in 2023.

There have been videos that incorporate snippets from the well-known television program *Kaun Banega Crorepati* in Madhya Pradesh. The snippets depict the quiz show, which stars Amitabh Bachchan, asking questions about Madhya Pradesh politics in an attempt to incite viewers' anti-incumbency feelings..

Since a phony film of Telugu star Rashmika Mandanna went viral earlier this month, deepfakes have been in the news in India. IT Minister Ashwini Vaishnaw called deepfakes a "threat to democracy," and PM Narendra Modi even voiced his worries about the technology's potentially harmful possibilities..

However, why don't political parties take strong action against phony films that disparage their candidates? The reason for this is because nearly all of the main parties have been involved in the deepfake propaganda industry.

6. Regulating Deepfakes:

From an Indian Point of View, in the legal system, victims of harmful deepfakes have few legal avenues for pursuing their claims. Criminal rules, both federally and in many states, are also not made to deal with chimeric nature of deepfake films, which show a person who is not genuine based on their specific face and physique. This analysis will focus on four separate causes of action: copyright infringement, right of publicity, defamation, and actions arising from non-consensual pornography laws. Due to the novelty of the technology, deepfakes bring to light a unique issue that raises several fundamental questions: Is it wrong to use a publicly available photo of a person's face and then creatively transform that photo into something else for a non-monetary purpose? Additionally, if the creation of deepfakes is wrong, would it still be wrong if the video was labeled as a work of fiction? Moreover, is the dissemination of a deepfake wrong if it is not defamatory? These questions are important because, unlike China, which outright prohibits the dissemination of false speech, the First Amendment protects citizens from the government attempting to ban content-based speech laws. Within the framework of the First Amendment, there are several possibilities by which the rampant and flagrantly malicious use of deepfakes can be curtailed. However, due to the technology behind deep fakes, some typical methods of curbing malicious media are not available. Collectively, these tendencies point to an exaggerated belief in the reach and pervasiveness of 'fake news' and misleadingly edited visual media, as well as an increased propensity for people to spread such content (Altay et al., 2022)[31], rising 'radical skepticism' in amplified experience, and diminishing trust in the media and civil rights (Chouliaraki, 2015)[32]. In order to better connect democratic accountability, reasonable and appropriate state-based legislation is required (Henry & Witt, 2021)[33], and to combat widespread problem of fake news and other information online, it is imperative that digital media be verifiably legitimate (Kietzmann et al., 2020; Khodabakhsh et al., 2019)[34].

a. Criminal statutes

India does not yet have any legislation or policies that specifically address deepfaked content. The closest are Sections 66D and 66E of Information Technology Act, 2000 ("IT Act"), which punish cheaters who impersonate someone and/or publish or send electronic photographs of a private area without consent with a fine and/or jail. In addition, people who post or transmit pornographic or sexually explicit content are prohibited and punished by Sections 67, 67A, and 67B of the IT Act.

Impersonation: Section 416 of the IPC makes impersonation a crime. Impersonation is defined in the section as posing as someone else with the intention of misleading. Impersonation carries a fine and a maximum sentence of three years in jail. Cheating: Section 415 of the IPC makes cheating a crime. According to this section, cheating is when someone is intentionally misled in order to persuade them to do or not do something. The seriousness of the violation determines the punishment for cheating, which can range from up to a year in jail to life in prison.

---

31 Altay, S. (2025, March 20). How Effective Are Interventions Against Misinformation?. https://doi.org/10.31234/osf.io/sm3vk_v2

32 Chouliaraki, L. (2015). Digital witnessing in conflict zones: The politics of remediation. Information, Communication & Society, 18(11), 1362–1377. https://doi.org/10.1080/ 1369118X.2015.1070890

33 Henry, N., & Witt, A. (2021). Governing image-based sexual abuse: Digital platform policies, tools, and practices. In J. Bailey, A., & N. Henry (Eds.), The Emerald inter national handbook of technology-facilitated violence and abuse (pp. 749–768). Emerald Publishing

34 Khodabakhsh, A., Ramachandra, R., & Busch, C. (2019). Subjective evaluation of media consumer vulnerability to fake audiovisual content. In Eleventh International Conference on Quality of Multimedia Experience (QoMEX), Berlin, Germany, 2019, pp. 1–6. https://doi.org/10.1109/ QoMEX.2019.8743316 , Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or treat? Business Horizons, 63(2), 135–146. https://doi.org/10.1016/j.bushor.2019.11. 006

Forgery: Forgery is an offense under Section 464 of IPC. Forgery is defined in the section as creating a fake document with the intention of misleading someone. Forgery has a maximum two-year jail sentence, a fine, or both.
Cybercrime: Cybercrime, including identity theft and fraud, is dealt with under the IT Act. According to the seriousness of the conduct, the Act lists a variety of punishments for different cybercrimes, such as fraud and identity theft, from up to three years in jail to up to 10 years.
Aadhaar Act: Indian citizens will have a unique identity system according to the Aadhaar Act of 2016. The Act also establishes penalties for a number of violations, including the improper use of Aadhaar, such as fraud and identity theft. It is crucial to remember that these legal rules are not all-inclusive; in some circumstances, additional laws may also apply. Additionally, the penalties for these offenses may vary depending on severity of offense committed.
However, these clauses are insufficient to solve the more significant issue of identifying and stopping the spread of harmful deepfaked information. The Union Government ("Union") appears enthusiastic to find a solution.
According to Section 354D of the Indian Penal Code, stalking is illegal. Stalking occurs when a male tries to contact a lady online without her consent using email, instant messaging, or any other electronic communication.
In addition, for reasons which will be discussed, simply prohibiting the creation of deepfakes might not actually practically solve issue of elucidating deepfakes from web (ibid). In essence, deepfake evidence is currently not particularly governed by any evidentiary approach, and the present legal criteria limiting evidence authenticity are inadequate. When dealing with deepfake evidence in court, judges and lawyers must avoid proof traps while also dealing with the prosecution's skepticism and mistrust (Delfino, 2022)[35]. Determining whether the deepfake was produced by humans or AI is another issue (Nema, 2021)[36].
Deepfakes and copyright laws in India
While it is true that India does not have a specific legislation to deal with deepfakes, copyright law is also not a way to handle grave problem of deepfakes.
Safe harbour protection has been given under Section 79 of Information Technology Act of 2000, which absolves social media companies of liability for information produced by third parties. However, after receiving notification from the government, its agency, or any individual, firms are compelled under Proviso 3(b) to remove or block access to the unlawful information; otherwise, they will no longer be protected.The four-factor test, which confirms fair use theory described in Section 107 of Digital Millennium Copyright Act of 1998 (DMCA), is the only prerequisite for removing copyrighted information in US. US law allows unlicensed use of protected content as long as the following requirements are satisfied:

- Effect of the use on the potential market.
- Nature of the copyrighted work.
- Purpose and character of the use.
- Amount and substantiality of the portion taken.

It's possible that deepfakes might be acceptable under the "fair use" concept and protected under the transformative perspectives principle.
The notion of fair dealing, as outlined in Section 52 of Copyright Act, 1957, is the equivalent of the "fair use" approach found in US law in India. This section outlined a comprehensive list of actions that are not considered to be infringing; deepfake content is not included in this list. The term "review" in Section 52(1)(a)(ii) of the ICA allows courts to adopt concept of transformative implementation as well as protect works that appear to benefit society as a whole, so even though this could be useful in slowing down maliciously created deepfake technology, it cannot protect utilization of deepfake technology for legitimate reasons. Authors are granted specific moral rights under Section 57 of the ICA to assert authorship of their work and to seek damages for any unauthorized conduct associated with it, including distortion, mutilation, alteration, and other acts.
According to Section 14 of the Copyright Act of 1957, the creators of a work that is protected by copyright have the only authority to do certain activities or grant permission to others to perform them in connection with their artistic, dramatic, or musical creations, sound recordings, or cinematic works.Civil and criminal responsibility remedies are provided by Sections 55 and 63 of the ICA, respectively. In the event that infringement is proven, the copyright owner may seek redress through rulings and injunctions that require the confiscation and destruction of illegal content.

Recommendations to tackle deepfakes

[35] Delfino, R. (2022). Deepfakes on trial: a Call to expand the trial Judge'S gatekeeping role to protect legal proceed ings from technological , fakery. Available at SSRN 4032094
[36] Nema, P. (2021). Understanding copyright issues entailing deepfakes in India. International Journal of Law and Information Technology, 29(3), 241–254. https://doi.org/ 10.1093/ijlit/eaab007

One obvious way to stop deepfakes is to implement rules and laws. Deepfakes are currently not covered by criminal legislation, especially in some countries. However, legal experts have suggested amending current regulations to include defamation, insults, personality crimes, and impersonating a politician using deepfakes. Deepfakes are now covered under Virginia's state legislation banning revenge pornography, which recently deemed the dissemination of phony images and videos to be illegal.

New types of rules and control structures are needed due to the increasingly complex AI technology. For example, because visual representation of people in deepfake films is not an exact replica of any existing content, deepfakes raise concerns about copyright and privacy; instead, they are novel depictions created by AI. Regulators need to search for a tough legal setting around free speech and possession rules to correctly control the employment of deepfake technology. However, a correct, lawful solution to the propagation of destructive deepfakes would not be to stop the technology completely, which is not lawful. Although new regulations can be made to prevent deepfakes, there should be ways to enforce them. Today's social network firms are well-protected against the content that users upload to their websites. One legal remedy would be to remove social media companies' legal immunity over content that their users consume. Deepfakes can be combated through education and training greatly. Though reasonable news has been presented by establishments, the public does not know or experience the consequences of deep fakes. Generally, the public has to be educated about the tendency of AI to be misused. Although deepfakes are novel instruments provided to digital fraudsters for social engineering, firms and establishments should be highly smart and create virtual resilience plans. Administrators, regulatory agencies, and individuals must recognize that, in contrast to appearances, video may not correctly depict events and be aware of the sensory cues that may be utilized to identify deepfakes. Children in school should be taught to think critically and creatively, as well as to be computer literate, so they can recognize fake information and interact politely with others online.

An anti-deepfake program has various ways and instruments used to

1) Identify deepfakes
2) validate material, and
3) help in preventing material from being utilized to create deepfakes.

Generally, this method cannot detect and validate fake content on a large scale. This is due to the fact that those who create deepfakes have access to more research materials than the technology that can identify them. On YouTube, for instance, individuals may upload 500 hours of content in a minute. Every week, Twitter battles 8 million addresses that attempt to disseminate false information. This makes it very difficult to check all the content uploaded quickly using technology. Also, deepfake producers seem to utilize works published on deepfakes to advance their program and know how to avoid being detected by novel detection technologies. Detection techniques that leverage fingerprints have emerged as one of the most promising methods to detect deepfakes. These techniques involve the analysis of small but unique traces left behind by the camera used to record the video, such as sensor noise, lens distortion, and emulated compression. Similar to fingerprints, these traces act as an identification system that is unique to each camera, and researchers have found that they are retained even after the deepfake is generated. By comparing the fingerprints of the original and deepfake video, it is possible to identify instances of deepfake content. These machine-learning-based techniques focus on minute differences among real and fake video content moreover, leverage fingerprinting approach to increase the accuracy of detection.

Discussion and conclusion

GANs involve an AI approach that can be easily used to construct deepfakes (Mirza & Osindero, 2014)[37], allowing for convincing human-mimicking audio and video content (Suwajanakorn et al., 2017)[38]. The average person may not have the tools necessary to spot a deepfake and avoid being tricked by one (R€ ossler, 2018)[39]. A new analysis of the moral, ethical, and psychological debate around deepfake technology is necessary because of its revolutionary nature (Farish, 2020)[40]. Deepfake technology may be used to take advantage of the political discourse and technological prowess that pervade our global media environment by creating a false social and political narrative (Cox & Williams, 2021; Slater & Rastogi, 2022)[41]. Both the 'knowledge impairment' of

[37] Mirza, M., & Osindero, S. (2014). Conditional generative adversarial nets. arXiv preprint arXiv:1411.1784.
[38] Suwajanakorn, S., Seitz, S. M., & Kemelmacher-Shlizerman, I. (2017). Synthesizing obama: learning lip sync from audio. ACM Transactions on Graphics, 36(4), 1–13. https://doi.org/10.1145/3072959.3073640
[39] Rossler, A. (2018). Faceforensics: A large-scale video dataset for forgery detection in human faces. arXiv preprint arXiv:1803.09179. Slater, K., & Rastogi, A. (2022). Deep-Rooted Images: Situating (Extra) institutional appropriations of deep fakes in the US and India. Fast Capitalism, 19(1), 93–101. https://doi.org/10.32855/fcapital.202201.007

[40] Farish, K. (2020). Do deepfakes pose a golden opportunity? Considering whether English law should adopt California's publicity right in the age of the deepfake. Journal of Intellectual Property Law & Practice, 15(1), 40 48. https://doi.org/10.1093/jiplp/jpz139

[41] Cox, J., & Williams, H. (2021). The unavoidable technology: How artificial intelligence can strengthen nuclear stability. The Washington Quarterly, 44(1), 69–85. https://doi. org/10.1080/0163660X.2021.1893019

deepfakes, which threatens credibility, moreover safety of first responders, and the responses to this 'disorder' carry risks, exacerbating existing inequalities (Gregory, 2021)[42]. There are potential epistemic promises and risks associated with deepfake technology that affect how we fare as enlightened individuals (Kerner & Risse, 2021)[43], and choices in the digital era may benefit more from a shift from instrumental to social rationality, which may be facilitated by Deepfake (Etienne, 2021)[44]. Advertising strategies, including creative development, media buying, and audience segmentation, are all susceptible to radical transformation in the face of deepfakes (Campbell et al., 2022)[45]. Existing literature on deepfakes suffers from a number of shortcomings, including problems with definition, insufficient demographic representation, and a lack of theoretical models (Vasist & Krishnan, 2022)[46]. Many of the issues that deepfake raises need, at least in theory, adjustments to the existing frame work of international law (Maas, 2019). The local environment and social setting are also crucial when analyzing deepfake and taking remedial actions (de Seta, 2021)[47].

[42] Gregory, S. (2021). Deepfakes, misinformation and disinfor mation and authenticity infrastructure responses: Impacts on frontline witnessing, distant witnessing, and civic journalism. Journalism, 23(3), 708–729. https://doi. org/10.1177/14648849211060644

[43] Kerner, C., & Risse, M. (2021). Beyond porn and discredita tion: Epistemic promises and perils of deepfake technol ogy in digital lifeworlds. Moral Philosophy and Politics, 8(1), 81–108. https://doi.org/10.1515/mopp-2020-0024

[44] Kerner, C., & Risse, M. (2021). Beyond porn and discredita tion: Epistemic promises and perils of deepfake technol ogy in digital lifeworlds. Moral Philosophy and Politics, 8(1), 81–108. https://doi.org/10.1515/mopp-2020-0024

[45] Campbell, C., Plangger, K., Sands, S., Kietzmann, J., & Bates, K. (2022). How deepfakes and artificial intelligence could reshape the advertising industry: The coming reality of AI fakes and their potential impact on consumer behavior. Journal of Advertising Research, 62(3), 241–251. https://doi.org/10.2501/JAR-2022-017

[46] Vasist, P. N., & Krishnan, S. (2022). Deepfakes: an integra tive review of the literature and an agenda for future research. Communications of the Association for Information Systems, 51(1), 590–636. https://doi.org/10. 17705/1CAIS.05126

[47] de Seta, G. (2021), "Huanlian, or changing faces: deepfakes on Chinese digital media platforms", Convergence, Vol. 27, doi: 10.1177/13548565211030185.