International Journal of Law, Social Science and Humanities (IJLSH)

Volume 3, Issue 2, 2026

E-ISSN: 3063-7554

https://doi.org/10.70193/ijlsh.v3i2.236

Exploring the Issues and Challenges of Deepfakes: A Doctrinal Study

Janees Rafiq[1*]

[1] Model Institute of Engineering and Technology, Jammu, J & K, India

Submitted: 03 June 2025 *Revised: 10 July 2026* *Published: 12 July 2026*

Abstract:

Technological innovation takes place every day. Every day, new breakthroughs in the field of technology continue to emerge. However, legislation has been unable to keep pace with such rapid developments; the laws currently in force in India and many other countries still lack specific provisions governing deepfakes. This study adopts a normative approach, focusing on legislation. The findings indicate that current guidelines may not be sufficient to address the challenges posed by deepfakes. To successfully combat harmful deepfakes, an integrated approach is required, involving the revision of provincial and federal legislation as well as cooperation with social media platforms and digital companies. Until appropriate legal provisions are enacted, media literacy may be the most effective way to address the negative impacts of deepfakes. It is also important to bear in mind that the development and use of deepfakes is an issue of international relevance; therefore, effective monitoring and the prevention of privacy breaches will most likely require international cooperation and coordination. During this transitional period, individuals and groups must be aware of the potential risks posed by deepfakes and exercise caution when verifying the authenticity of content received digitally.

Keywords: Exploring; Issues; Challenges; Deepfakes; Doctrinal Study

INTRODUCTION

Substantial advances in technology in the past few decades have allowed the production of content for specific categories of individuals (Togle, 2026). Some of these changes offer worries revolving around misinformation, particularly, differentiating between accurate and misleading information. The deliberate creation of untrue information from media outlets that are sent to a consumer's feed along with real-time information is a particular kind of false information activity that might negatively impact a large portion of social media platforms (Brown, 2019).

Fake photographs exist on the internet nowadays, and they appear to be harmless. We have undoubtedly witnessed the 'Face Swapping' features on Snapchat, or other such applications, where the users are allowed to change a person's face with someone else (Hatta, 2020). Most of the audience have also been a part of the 'age yourself' trend and see what they would look like during their old age. Apart from the fact that such applications are invented solely for entertainment, they are largely innocent since an individual can easily detect the difference between whether it is real or fake. This is the only reason why deepfakes are hazardous because they result in such images, which makes it impossible for normal human beings to recognize the difference between real and fiction (UVA Information Security, 2026).

People have been manually and digitally manipulating and modifying videos and pictures for Deepfakes, irrespective of whether we recognize them or not, have already become a significant

*Corresponding Author : Janees Rafiq, Model Institute of Engineering and Technology, Jammu, J & K, India, ORCID iD: 0000-0002-4907-1008, E-mail: janees.llb@mietjammu.in.

component of our everyday lives, as their usage on social networking sites, politics, the arts, and various other fields grows frequently (Finklea, 2012). Aside from the troubling sexual abuse characteristics of deepfake technology, deepfakes were also used for enjoyment, training, and exploration in Hollywood, online forums, and the realm of politic (Mullen, 2022). Deepfakes are an innovative and successful method for spreading lies (Rahman & Anggriawan, 2025). Their influence is calculated not only based on how convincing they are but also regarding their timeliness and authenticity of the disapproval of a deepfake.

METHODS

This study is a normative study employing a statutory approach. This normative legal study on deepfake crime in India focuses on legal gaps. The study highlights that India does not yet have specific legislation criminalising synthetic media, meaning that law enforcement must rely on cyber and general criminal laws, which are reactive and inadequate (Chang, 2024). The data sources for this normative legal research on deepfake crime focus on the analysis of library materials, legislation and legal literature. (Christiani, 2016) As normative research does not utilise field data (such as interviews or questionnaires), the data is classified.

Data processing techniques for normative research on deepfake crime involve the stages of inventorying, classifying and systematising legal materials (Noor, 2023). Qualitative data is analysed descriptively and analytically using methods of legal interpretation (such as grammatical, teleological and systematic approaches) to address legal vacuums and harmonise legal norms or resolve legal issues relating to deepfake crime (R.C Bogdan & S.K Biklen, 2025).

RESULTS

Deepfake and Information Technology Act

Section 66D of the Information Technology Act of 2000 states that "Whoever utilizes a communication means or computer system to commit impersonation-related fraud will be liable to give a fine of up to one lakh rupees along with an imprisonment period that goes up to three years."

Section 66E of the Information Technology Act of 2000 states that, "Any person who, deliberately or carelessly, clicks an image of an individual's private area/part without taking permission from the concerned person, then that breaches their right to privacy and is liable to face up to three years of imprisonment, or a fine of up to two lakh rupees, or it can be both depending on the judicial decision."

For the purpose of this regulation under the act, the term:

a. Transmit means sharing a visual image through electronic means with the intent to be viewed by one or more individuals.

b. Publishes refers to duplicating anything in print mode or electronic form to make it accessible and visible to the masses.

c. Conditions that infringe the privacy are those in which an individual can reasonably expect that:

    1) He or she can undress in privacy, without being concerned that an intimate image is being captured.

    2) Any part of his/her private image will not be shown to the public, notwithstanding whether that person is in a public or private space.

Section 67 of the Information Technology Act of 2000 states that:

a. Anyone who transfers, releases, or leads to be distributed in electronic form any inappropriate or sexual material that appeals to an individual's lustful interest, or if it has the effect of promoting wicked and immoral individuals who are likely, taking into account all related elements, to read, see, or hear the data included or displayed in it, encounters penalty. The punishment goes up to

five years of imprisonment as well as a fine of about one lakh rupees. And for subsequent conviction, it can be two lakh rupees or ten years in jail.

b. Further, Section 67A of the Information Technology Act of 2000 stipulates that "Whoever publishes or transmits in the electronic form any content which incorporates sexually explicit acts will be penalized with imprisonment for a term which may go up to five years and with a fine up to ten lakh rupees and in circumstances of a second conviction, the imprisonment can go up to seven years and fine of ten lakhs rupees."

c. Additionally, Section 67B of the Information Technology Act of 2000 punishes "the act of publishing, transmitting or causing to do both via electronic means or creating text/images/videos/digital images of the children engaged in sexual acts, encouraging abuse of the children over the internet, recording sexual abuse of children through the electronic medium will be punished with five years of imprisonment and ten lakhs' rupees fine."

In response to the growing concern about deepfake challenges, the Government of India adopted a multifaceted approach, drafting rules and regulations that will punish not only the people who are responsible for posting false content but also the social media systems that publish it.

Deepfake and Copyright Law

Sometimes deepfakes include pirated copyright content, which could result in infringement claims. The copyrighted content could be anything ranging from a broadcast interview with a politician or a short still from a movie. It is the person who shot the photograph, not the person depicted in it, who owns the copyright (Nagumotu, 2022).

The rules and regulations addressing deepfakes often disregard intellectual property issues. Some might erroneously believe that the current copyright protection can be employed to battle deepfakes. However, it is critical to emphasize that copyright regulations differ from one jurisdiction to another and may not necessarily safeguard against deepfake violations (Hussain, 2023).

Deepfake videos frequently involve corrupted or fabricated replicas of sound or visual recordings obtained from a film or movie that could be copyrighted assets. Section 14 of the Copyright Act of 1957 stipulates that the owner of the copyright of a cinematographic film and audio recording has the sole permission to do or license making a copy of the film, that includes a photograph of any image becoming part thereof, or making any additional sound recording demonstrating it, correspondingly.

In India, the principle of *fair dealing* as stipulated under *Section 52 of the Indian Copyright Act 1957* regulates which works are exempt from being considered copyright violations. Unlike the procedure adopted by the United States, the notion of fair dealing in India constitutes an exception to copyright infringement. The legislation provides a list of actions that are not included in the violation of intellectual property.

While others perceive India's strategy as rigid, it is effective when confronting deepfake technology since this kind of use is not covered within any of the operations outlined in Section 52 of the Indian Copyright Act, 1957. It follows Article 13 of the Trade-Related Aspects of Intellectual Property Rights (TRIPS), which stipulates that "Members must restrict limitations or exceptions to exclusive ownership to a few unique circumstances that are not inconsistent with the normal exploitation of the creation and do not unfairly prejudice the rightful interests of the right holder."

Since deep fakes depend on the reusing of existing copyrighted content such as pictures and movies this type of usage is instantly deemed an infringement of copyright protection as it fails to appear in the works protected by law. This prohibition is especially severe as it limits the utilization of deep fake technology for whatever reason, legitimate or otherwise (Satheesh, 2025). However, the malicious use of the same has currently surpassed its benefits, hence the researcher believes that it is a correct state of practice.

Section 57 of the ICA offers people the right to integrity, in keeping with the liberties established by the Berne Convention of 1886. Whenever it comes to deepfakes, the right to integrity contained in

Section 57(1), (b) of the ICA arises because deep fakes are occasionally thought of as deformations, mutilations, or alterations of the work of another individual.

However, the problem again arises concerning the fact that what if such alteration produces a novel work (BA, 2011). Will that be brought within the domain of copyright protection or be declared as copyright infringement, continues to remain a mystery.

DISCUSSION

Deep Fake Technology

From its humble beginnings in the mid-1990s to the advent of a widely utilized application in 2018, deepfake technology has evolved in competence while becoming accessible to the public at large. "Deepfake", a fusion of the terms "deep learning" and "fake" is a sort of artificially produced media in which artificial intelligence is implemented to generate an electronic duplicate of an individual's image or sound (Zulfan, 2024).

Around 2017, an anonymous Reddit user who named himself "Deepfake" claimed to be the creator of videos that utilized the faces of celebrities or renowned persons and placed them on pornographic videos and pictures. The post shared by the user became increasingly famous globally. A specialized page was created under the Reddit page, which came to be referred to by the name "*subreddit*". It was dedicated particularly to deepfake videos and hence instantly came under the view of a large audience. A deepfake is simply a video through which hyper-realistic faces are glued onto the bodies of other individuals to develop a novel video with forged depictions. It is a type of AI-invented synthetic content that switches a person's audio, video, or image with another person.

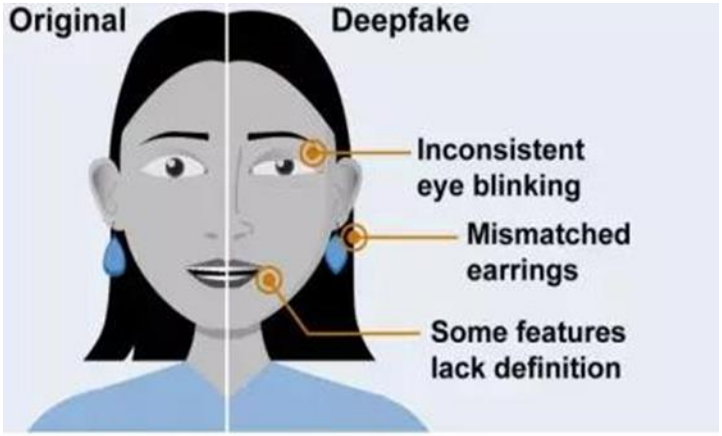

Figure 1. Depicts the difference between the original picture and a deepfake image

Deepfakes have derived their designation from the technology employed to generate bogus content i.e. deep learning. Deep learning is a small portion of machine learning technology that analyses, identifies, discovers data, and subsequently generates patterns by utilizing numerous layers of networks. Deepfake technology which relies upon Artificial Intelligence to produce electronically modified audio, videos, and pictures that look trustworthy, has subsequently advanced and is now skilled in developing multimedia content that is more challenging to distinguish from authentic recordings.

Deepfakes Operate

The approach most employed to generate deepfakes is to use *Generative Adversarial Networks* (GANs), which originally appeared in the year 2014. A GAN comprises two competitions (ANNs): one network, identified as the generator, obtains a hidden sample and produces an image out of it. The

result of this training is subsequently fed into another network, identified as the discriminator, which was successfully developed on real data to recognize differences between actual and phony images.

The machine that discriminates rates the deception on an index of zero to one, with one indicating an elevated likelihood that the image is legitimate and zero illustrating a high chance that the image is unreal (Davis et al., 2020). The generator changes its weights depending on the evaluation and feedback up until the discriminator can hardly tell the disparity between the falsification (generator output) and an actual picture.

Another different technique for deepfake generation employs *Variational Autoencoders* (VAEs). Unlike adversarial networks, VAEs are generative frameworks that rely on two distinct networks' collaboration. The encoder network produces a lesser and thicker version of the provided data, which the decoder utilizes to reproduce the initial data.

These networks undergo conditioning jointly on a single set of data, such as dozens of pictures of a famous person, until both the input and the output are approximately coordinated. Following that, the decoder can be modified to accomplish the desired operation, for instance, adding spectacles to a particular target from the initial AV media.

Types of Deepfakes

There exists no list for the set of deepfakes, the environment is now filled with varied kinds and hence some of them are discussed below:

Face Swaps

Face recognition software detects or confirms an individual by evaluating the distinctive characteristics of face areas while contrasting them to known patterns. Such methods are regularly used and refined in many applications since they are customer-friendly, not intrusive, clear, and economically efficient, enabling facial images to be gathered quickly through a wide range of accessible apparatus (Sundström, 2023).

However, such an easy-to-collect character increases the likelihood that face data could easily slip into unauthorized hands and be used maliciously. The results are extremely genuine, and in certain instances challenging for a human inspector to recognize. An attacker may additionally generate demeaning data to accomplish intimidation targets or to affect the public's impression of a particular individual or political figure. The method may also be employed to manipulate with security film or different sorts of historical documents to plant fabricated proof in a legal proceeding.

Textual Deepfake

The expression 'textual deepfake' can indicate the use of advanced natural language processing, or NLP, and machine learning methods to generate persuasive and deceptive written material. It could entail developing counterfeit writings, feedback, or interactions that duplicate a particular person's manner of writing or pretend to be representing an authentic source.

Textual deepfakes resemble human-written documents and may be employed to spread erroneous data. This kind of subject matter, especially those posted on social networking sites, is viewed as an imminent risk with the ability to have an important impact on civilization due to its fast and widespread propagation (Malik & Choudhury, 2019).

WIRED has described AI-generated text as 'the deadliest deepfake of all,' showcasing one of the most effective text producers accessible: OpenAI's Generative Pre-Trained Transformer (GPT-3) language model. GPT-3 is an autoregressive model of language that relies on deep learning to produce writings like human beings.

Simply put, GPT-3 has been tasked with analyzing statistical patterns in a data set of around a trillion phrases extracted from the web and digital publications. GPT-3 then employs its summary of that enormous database to react to text requests by generating novel content with equivalent analytical patterns, giving it the ability to create fresh stories, rhetorical information, and even songs and poems (Simone, 2021).

Audio Deepfake/Voice Cloning

An audio deepfake is a type of artificial intelligence that produces compelling spoken phrases that appear like specific people communicating things they did not utter. The technology in question initially emerged for an array of purposes that focused on enhancing the quality of life for people. For instance, it could be used for producing e-books and to help people who have lost their ability to speak. On a commercial level, it gave rise to multiple opportunities.

Audio deepfake based on copying is an approach that transforms a genuine voice from a single individual (the source) to one that sounds like another individual (the target). An imitation-based system receives a spoken message as input and changes it by altering its syntax, pronunciation, or language to sound like the intended voice without destroying its semantic content. It is occasionally referred to as voice conversion.

In the opinion of experts, audio deepfakes have grown into an increasingly prevalent type of deceit as startups such as ElevenLabs, Resemble AI, Respeecher, and Replica Studios develop inexpensive, yet outstanding performance-giving artificial intelligence (AI) tools. Audio deepfakes are becoming increasingly common. The methods use artificial intelligence for analyzing audio information, detecting the characteristics and patterns of a target speech, and then producing a replica of that voice which can say anything the developer desires.

While it was initially meant to generate benefits, the technology has now progressively been employed for malevolent purposes. Audio deepfakes can be effortlessly constructed and more challenging to identify than visual deepfakes. Audiences have less context-based information while listening to a recording as compared to when observing a video clip, where uncommon movements of the face, apparent problems, or incorrect physiological or background components might notify an observer (Alert, 2024).

In the year 2019, scammers employed voice cloning technology to take advantage of a UK-based energy service provider. In a phone conversation, the con artist claimed to be the chief executive officer of the company's German parent business, demanding an urgent payment of 243,000 dollars to the bank account of an identified supply organization.

After the funds reached their destination, the scam artist reached a second time, first to reassure the UK office staff that the parent company had previously sent a refund and then to try to arrange further transfer. At all three times, the UK CEO was sure he was speaking with his superior since he identified both his German dialect and additionally his language and manner of speech. The second payment wasn't transmitted as the scammer reached out from an Austrian landline instead of a German one, which sparked questions with the UK SEO (Anikin, 2025).

Deepfakes & Right to Privacy

In democratic traditions, there is an essential belief in each person's individuality, respect, and worth as a human being. Both sociologists and psychologists have linked the development and conservation of a sense of self-worth to the human need for independence. One suitable approach for expressing an individual's desire for a final base of liberty has been to describe an individual's interactions with others in terms of an order of areas or regions of privacy that eventually lead to a '*core self*'.

The core of oneself appears as wrapped by a sequence of consecutive rings. The inner group protects the person's biggest confidential information, those objectives, worries, and ambitions that are beyond discussion with anybody until the person in question is under such strain that he has to disclose his ultimate secrets for the reason to find mental comfort.

The greatest risk to human autonomy is that someone might get into this innermost zone and pick up its greatest secrets, through physical contact or by other means. This deliberate entering of an individual's protective shell, his psychic armour, subjects him to mockery and places him under the authority of others who know his secrets.

Do you sometimes sense that you are being observed? In the current era of ongoing electronic surveillance and unethical data collection strategies, that sneaking understanding is more accurate than we know. Artificial intelligence has allowed the production of deepfakes-fabricated photos, sounds, recordings, and videos that look and feel alarmingly authentic. Deepfake software is growing increasingly advanced and widely available, presenting an enormous risk to confidentiality and safety.

A study conducted by the Berkman Klein Center for Internet & Society at Harvard University provided certain regulatory ethical principles for the Artificial Intelligence One of the most prevalent standards is privacy, which calls for the preservation of confidentiality. Responsibility for the implications of actions, along with the provision of appropriate treatments, is a common desire. AI security and reliability are of the highest priority for the sake of its desired performance and endurance to invasions.

The fourth set of characteristics is transparency and simplicity, which demand understanding and visibility of methods, outcomes, and implementations. Equality and non-discrimination require AI systems to be inclusive and promote equitable societies, as expressed in all texts examined. Professional accountability demands individuals involved in the advancement of AI to be able to foresee the effects of their decisions. artificial intelligence ought to improve mankind's wellness.

Any illegal construction of a photograph, audio, or video snippet for marketing purposes is an intrusion of privacy. Dissemination of other offensive or humiliating content may additionally be regarded as a violation of privacy rights if the delivery is carried out in a way that might deceive the public regarding the person portrayed in them.

Right to Informational Privacy

The most hilarious aspect of the right to privacy is that nobody has a clear idea of who and what it encompasses within its domain. In 1977, the United States Supreme Court in the case of Whalen v Roe (429 U.S. 589 (1977), recognized two distinct kinds of privacy in its jurisprudence. A group of medical professionals and patients contested a New York legislation that demanded the gathering and consolidation of all Schedule II medication prescriptions in a computerized database.

A few patients protested, reluctant that their identities might be disclosed, leading them to be labeled as drug addicts. Furthermore, those receiving treatment claimed that their fear of exposure would stop them from utilizing treatments covered by the law, even if they were compelled because of their health.

The Court separated the privacy contentions into two major groups: One is a person's desire to avoid revealing sensitive data, and the other is the need for autonomy when making a couple of important judgments. Informational privacy is frequently referred to as the confidentiality limb of the right to privacy. It denotes the desire to thwart disclosure. The interest in making certain important choices is better known as *Decisional privacy*, or the autonomy branch.

A nine-judge bench of the Supreme Court of India in the case of *Justice K. S. Puttaswamy and Anr. vs Union of India and Ors* ((2017) 10 SCC 1) held that the "Right to Privacy is a fundamental right protected under Part III and specifically Article 21 of the constitution." The court highlighted that privacy is inseparably connected to an individual's ability to govern his or her distinctness.

The benefit of any associated security measures in Part III is dependent on preserving the right to privacy. The fundamental right to privacy ought to encompass at least three components: (i) invasion of an individual's bodily integrity, (ii) confidentiality of information, and (iii) freedom of selection..

Justice Nariman was of the view that *"Information privacy pertains to an individual's mental state as opposed to his body; therefore, it recognizes that a person could exercise influence over the dissemination of sensitive data. Illegal use of this kind of data could end in the violation of the afore-mentioned right.*"

Justice Chandrachud while delivering judgment mentioned that *"In Second Treatise of Government published in 1690, John Locke argued that individual lives, liberties, and possessions are a personal*

deposit under fundamental natural law." The objective of an exclusive reserve was to construct limitations towards external interference. Privacy respects the independence of individuals and the right of everybody to make substantial choices that influence the course of their respective lives.

In the informational era, challenges against confidentiality may emanate from both the government and outside actors. The setting up of a privacy system requires an intricate equilibrium between individual desires and the government's righteous worries. A person's capacity to control his or her private information and to live in their way encompasses the right to exercise control over his or her online existence.

Individuals showcased in deepfake audio/images/video often do not consent to having their appearance taken advantage of in such a way. The absence of authorization compromises the regulation of the individual regarding their private information and their willingness to guard their privacy rights. The user's right to have authority over their personal and sensitive information has been materially diminished due to the growing popularity of deepfake technology.

Therefore, any person with modest technical knowledge and the right equipment can now produce and alter the real content with the view to disseminating false information by using real information and easily annoying others. Our pictures and audio-video recordings can be utilized without authorization to create deepfake content. We have stepped into an era where survival depends on questioning what is real and what is not.

In a nutshell the nonconsensual publication or dissemination of a photograph or video snap that was intentionally forged using technological devices in order so that it can be believed to be genuine, and which can degrade and denigrate the individual who is depicted in it, or includes data purportedly associated to his private life, qualifies as an abuse of the right to privacy, including right to information confidentiality.

Right to Bodily/Sexual Privacy

Sexual privacy pertains to the covering of unclothed bodies as well as private acts, involving but not restricted to sexual activity. It includes individual choices regarding close relationships, such as whether to share details regarding a person's sexual orientation or gender with other people, or whether to expose a person's body to others. Sexual privacy is critical for the exercise of individual freedom and sexual independence.

Nonconsensual deepfake pornography is an assault on the idea that individual personal identification is private to disclose or preserve to themselves, comparable to the nonconsensual revelation of pornography that demonstrates an individual participating in actions they conduct.

Though deepfakes avoid showing an individual's nude body, only the face of the subject is utilized, they nonetheless breach sexual independence by repurposing the recipient's identity. The fundamental problem with nonconsensual pornography is authorization, and deepfake pornography introduces an additional aspect because the individual who is shown did not indulge in the sexual conduct displayed.

Deepfakes are hyper-realistic pictures in which an individual's face is examined by an algorithm using Deep Learning and positioned above the face of a performer in a clip. Because the machine learning system has acquired facial characteristics from multiple viewpoints as well as how it shifts in different gestures, it could reconstruct them in a way that is comparable to the actor's expression.

The development of instruments such as *FaceApp* allowed novices and aficionados to create their Deepfake films utilizing the application and video footage from the individual whose face they were interested in using. While this possibly makes everybody a target of Deepfake Pornography, the phenomenon looks to be strongly gendered. Like other pornographic material, it is mainly produced by and for male consumers, albeit (fictitiously) starring women who have not provided permission to participate.

Thus, in the beginning, the law limited itself to punishments for physically interfering with property and life. The right to life then worked merely to safeguard life from various types of battery; freedom

meant independence from practical restrictions, and the property right ensured an individual's land and cattle; subsequently, there was consciousness of the spiritual aspect of his sentiments and intelligence.

Tussle between Deepfake and Personality Rights

Personality rights pertain to an individual's capacity to protect their own identity through the right to privacy or property. Artists and dignitaries honour these rights since their identities, images, and even sounds may be employed erroneously in marketing by various companies to enhance revenue. For the sake of their rights, honoured persons and superstars may seek legal relief in a court of law. In India, the statutory remedy for safeguarding personality rights is Article 21 of the Indian Constitution, which protects the right to life and dignity, including anonymity and publicity.

The right of publicity evolved from the right of privacy and can exist solely in an individual or any evidence of the identity of a person, such as his legal name, character attribute, signature, pronunciation, etc. A person can gain the right of publicity using his affiliation with an event, athletic endeavour, motion picture, etc. No identity can be monopolized. People have the right to advertise themselves, which means they are the sole individuals who can benefit from it.

Personality rights provide an individual an opportunity to regulate the commercial utilization of his or her name, personality traits, or speech. Consequently, individuals get protection from undesired exposure in the community while additionally guaranteeing prior permission has been acquired for usage. For instance, if an online game is based on a famous person, the individual ought to possess the right to agree to the utilization of his digital illustration in the game.

The right to publicity includes the ability to defend, supervise, and capitalize on one's image, designation, or likeness. This liberty is frequently interpreted as an integral part of the right to privacy. There are two separate components of publicity rights: the ability to prohibit one's image from being economically used without authorization, which is regarded as a tort of passing off; and the right to privacy, which involves the right to be left alone.

In *Haelan Laboratories Inc v Topps Chewing Gum Inc* (202 F.2d 866 (2d Cir. 1953), the court stated that "every person should be given the right to maintain control over his or her private affairs and appearance as presented to the outside world, and also to regulate the commercial use of his/her reputation. This in addition suggests that a person may be able to forbid others from employing his or her image, identity, and other components of his or her private identity and life for commercial purposes without his or her approval."

Although no express law, legal enactment, law, or regulation aims to safeguard personality rights, the Indian judiciary has made an effort to construct the same from Articles 19(1)(a) and 21 of the Indian Constitution, which deal with the freedom of 'expression' and the right to live with dignity, respectively, in conjunction with Indian Intellectual Property Rights (IPR) laws.

An interesting case of clever yet not-so-subtle use of a person's name, or rather an infringement of a person's personality rights, is perhaps *Shivaji Rao Gaikwad v Varsha Production* (2015 SCC OnLine Mad 158), wherein prominent celebrity Mr. Shivaji Rao Gaikwad otherwise known as "Rajnikanth" felt obligated to approach the Hon'ble Madras High Court looking for an injunction preventing a production house from utilizing his name, illustration, manner of dialogue delivery, and so on in its forthcoming film 'Main Hoon Rajinikanth'.

Surprisingly, not merely was the name and acting style of the mentioned dissatisfied celebrity utilized without explicit permission or approval, but the name of the afore-mentioned film also unmistakably indicated that it addressed Mr. Rajnikanth. The Hon'ble Madras High Court granted the injunction as asked for, detailing that, following Article 21 of the Constitution, every person has the right to live a life of dignity, and thus any harm to a person's credibility and persona would be negative to the legitimate interests of the law, with adverse repercussions for the plaintiff.

The fundamental elements of responsibility for infringement of the right of publicity are:

a. Validity: The Plaintiff possesses an actionable interest in the identity or personality of a human.

b. Identifiability: The Superstar must be recognizable by the accused person's illegal use. Violation of the right to publicity requires no proof of untruth, misunderstandings, or deceit, especially once the celebrity has been recognized. The right to publicity goes above the usual application of deceptive marketing rules and regulations.

Mr. Amitabh Bachchan, an acclaimed actor, lodged a lawsuit against the defendants alleging an infringement of his personality rights as an eminent individual in the case of *Amitabh Bachchan v Rajat Nagi and Ors* **(**CS(COMM) 819/2022) The defendants mainly misused portions of his individuality, such as his pictures and voice, to tempt the public to browse and/or install their mobile applications, websites, and merchandise. For example, one defendant used the victim's recognized profile for executing a KBC Lotteries fraud, whereas another distributed t-shirts with the plaintiff's representation on his website. The court decided that the complainant was able to present a compelling prima facie argument in its support. The Court directed an ad interim ex parte injunction against the known and anonymous defendants after concluding that the plaintiff is likely to experience severe irreversible damage and harm to his image as a result of such illicit usage.

The court additionally directed the Department of Telecommunications and the Union Ministry of Electronics and Information Technology to eliminate the list of hyperlinks and websites breaking on the plaintiff's personality rights, and it also ordered telecommunications companies to disable all contact numbers used to circulate statements through WhatsApp that contravened the plaintiff's rights.

Recently, the Hon'ble Delhi High Court in the case of *Anil Kapoor v Simply Life India and Ors* (CS(COMM) 652/2023) took a comprehensive approach and restricted the respondents from 'utilizing his identity, picture, speech, likeliness, or character' to make any goods, ringtones or in any way abuse the petitioner's designation, sound, and various other elements by using technological instruments such as artificial intelligence (AI), face transforming, animated images (GIF) either for revenue generation or for building video content for advertising purposes. The primary separating characteristic is the extent and the scope of advertising of individual rights without delivering any charges to the superstar. The security of personality rights granted in the *Anil Kapoor case* also addressed the contested question of exercising the freedom of expression and speech under Article 19(1)(a) in conjunction with the use of celebrity identities and visuals, among several other issues.

It has been established that free expression does not encompass the monetization of an individual's personality and that the non-voluntary use of such a person's name, image, and likeliness is also a serious violation of their right to privacy (Nkoane, 2026). Personality rights are reminiscent of an individual's means of livelihood. As a consequence, the unlicensed and illicit utilization of any celebrity's personality is an immediate threat to their ability to survive.

It was held by the court that, 'Using an individual's name, speech, dialogue, or face illegally, particularly for financial gain, is not authorized.' The stars' endorsement rights could constitute an essential source of revenue for them, which may not be completely eradicated by marketing goods, etc (Petrus Sihombing, 2026).

It is therefore essential that straightforward and comprehensive legislation be created that clearly defines personality rights as an instance of unique intellectual property and permits for commercial registration so that the person can benefit financially from the use of their personality and likeness, while simultaneously supporting invention as well as accountable advertising procedures.

CONCLUSION

As Winston Churchill once said, '*A lie may travel around the world before what is true is identified*.' Whether technology firms make modifications or investigators and other reporters make breakthroughs, people who seek to deceive will change with them. Deception is an epidemic that must be constantly tracked and tailored to, similar to crime.

Innovations in technology occur every single day. Each day a breakthrough in technology emerges. Nevertheless, legislation fails to change at such a rapid pace, present-day laws in India and multiple

other countries are lacking legislation especially regulating deepfakes. The currently in-place guidelines can fail to be appropriate for resolving deepfake challenges.

It is surpassing identification endeavors. Nevertheless, even a blanket ban on deepfake material could restrict the freedom of speech. Hence, harmony needs to be established between the protection of the fundamental right of freedom of speech and expression and also safeguarding individuals from the threat posed by deepfake technology.

The only logical assumption is that deepfakes imply risk. As demand for the method of production rises, deepfakes will grow in excellence, become progressively less expensive and easier to produce, and be spread thoroughly across both commercial enterprises and the illegal auction sites of the Dark Web, wherein deepfake generation is anticipated to begin operating as an occupation.

The final outcome will be an upsurge of fake but extremely plausible multimedia information, prepared to be exploited for political ends and circulated on social media. To successfully combat malicious deepfakes, an integrated approach is required, involving revising provincial and federal laws and collaborating with social networking sites and Digital firms. Until appropriate legal provisions are put in place, media literacy might serve as the most effective way to deal with deepfake injuries.

It is also important to remember that the development and application of deepfakes is an internationally relevant problem, so successful monitoring and avoidance of privacy violations will probably require international collaboration as well as coordination. In the interim period, individuals and groups ought to be aware of prospective risks posed by deepfakes and be careful in verifying the veracity of content received digitally.

Conflict of Interest

All the authors declare that there are no conflicts of interest.

Funding

This study received no external funding.

How to cite:

Rafiq, J. (2026). Exploring the Issues and Challenges of Deepfakes: A Doctrinal Study. *International Journal of Law, Social Science and Humanities (IJLSH)*, *3*(2), 505-517. https://doi.org/10.70193/ijlsh.v3i2.236.

REFERENCES

Alert, C. (2024). *Audio Deepfakes: Cutting-Edge Tech with Cutting-Edge Risks*. Https://Www.Bradley.Com. https://www.bradley.com/insights/publications/2024/01/audio-deepfakes-cutting-edge-tech-with-cutting-edge-risks

Anikin, D. (2025). *Don't Believe Your Ears: Voice Deepfakes*. Https://Www.Kaspersky.Co.Uk. https://www.kaspersky.co.uk/blog/audio-deepfake-technology/26223/

BA, C. E. P. (2011). *An Analysis Of Evidence-Based Medicine In Context Of Medical Negligence Litigation* (Vol. 1, Number 2). University of Pretoria.

Brown, R. (2019). *Public Relations and the Social Web: Using Social Media and Web 2.0 in Communication*. Kogan Page.

Chang, Y. (2024). The Empirical Foundation of Normative Arguments in Legal Reasoning. *European Journal of Empirical Legal Studies*, *1*(1), 69–88. https://doi.org/https://doi.org/10.62355/ejels.18070

Christiani, T. A. (2016). Normative and Empirical Research Methods: Their Usefulness and

Relevance in the Study of Law as an Object. *Procedia-Social and Behavioral Sciences*, *219*, 201–207. https://doi.org/http://dx.doi.org/10.1016/j.sbspro.2016.05.006

Davis, R., Wiggins, C., & Donovan, J. (2020). *Deepfakes*. Belfer Center for Science and International Affairs.

Finklea, K. M. (2012). The Interplay of Borders, Turf, Cyberspace, and Jurisdiction: Issues Confronting U.S. Law Enforcement. *Journal of Current Issues in Crime, Law & Law Enforcement*, *5*(1/2), 13–20.

Hatta, M. (2020). Efforts to Overcome Cyber Crime Actions in Indonesia. *International Journal of Psychosocial Rehabilitation*, *24*(3), 1761–1768. https://doi.org/10.37200/IJPR/V24I3/PR200925

Hussain, A. (2023). DeepFakes: A Challenge to Copyright Law. *Jus Corpus Law Journal*, *3*(249), 546.

Malik, J. K., & Choudhury, S. (2019). A Brief Review on Cyber Crime-Growth and Evolution. *Pramana Research Journal*, *9*(3), 242.

Mullen, M. (2022). A New Reality: Deepfake Technology and the World Around Us. *Mitchell Hamline Law Review*, *48*(1).

Nagumotu, K. (2022). Deepfakes Are Taking Over Social Media: Can the Law Keep Up?'. *Journal of The Franklin Pierce Center for Intellectual Property*, *62*(102).

Nkoane, L. (2026). Public Participation in Municipal Planning and Development: South African Local Government Perspective. *International Journal of Law, Social Science, and Humanities (IJLSH)*, *3*(2), 494–504. https://doi.org/https://doi.org/10.70193/ijlsh.v3i2.225

Noor, A. (2023). Socio-Legal Research: Integration of Normative and Empirical Juridical Research in Legal Research. *Jurnal Ilmiah Dunia Hukum*, *7*(2), 94 – 112. https://doi.org/https://doi.org/10.35973/jidh.v7i2.3154

Petrus Sihombing, & I. S. (2026). The Illusion of Oversight: Fragmented Governance and Weak Legal Enforcement of Marine Environmental Degradation Caused by Nickel Mining Activities in North Kolaka. *International Journal of Law, Social Science, and Humanities*, *3*(2), 473–493. https://doi.org/https://doi.org/10.70193/ijlsh.v3i2.309

R.C Bogdan & S.K Biklen. (2025). *Qualitative Research for Education*. Allyn and Bacon.

Rahman, R. A., & Anggriawan, R. (2025). Deepfake and Electoral Crimes: Criminal Law Perspectives from Indonesia, India, Pakistan, and the U.S. *Ndonesian Comparative Law Review*, *7*(2). https://doi.org/https://doi.org/10.18196/iclr.v7i2.26337

Satheesh, A. (2025). *Deepfakes and the Copyright Connection: Analysing the Adequacy of the Present Machinery*. Https://Jolt.Richmond.Edu. https://jolt.richmond.edu/2022/01/25/deepfakes-and-the-copyright-connection-analysing-the-adequacy-of-the-present-machinery/

Simone, M. (2021). The scariest deepfake of all: AI-generated Text and GPT3. *Bowdoin Science Journal*, *1*, 203.

Sundström, I. (2023). *Deepfake detection by humans: Face swap versus lip sync*. KTH Royal Institute of Technology.

Togle, G. M. A. (2026). Challenges, Acceptance, and Adoption of Electronic Payment at Teodoro Arcenas Trade Center Towards Efficient Local Development. *International Journal of Law, Social Science, and Humanities*, *3*(2), 451–459. https://doi.org/https://doi.org/10.70193/ijlsh.v3i2.306

UVA Information Security. (2026). *What the heck is a deepfake?* Https://Security.Virginia.Edu. https://security.virginia.edu/deepfakes

Zulfan. (2024). Cybercrime in Virtual Spaces: An Overview of the Law in Indonesia. *International Journal of Law, Social Science, and Humanities (IJLSH)*, *1*(1), 18–26. https://doi.org/https://doi.org/10.70193/ijlsh.v1i1.140