



Deepfakes: Concept, Celebrity Instances, Impact and related Indian and U.S. Laws

Akanksha Singh¹, Dr. Manish Kumar Singh²

¹Research Scholar, NIMS School of Law, NIMS University Rajasthan, Jaipur

²HOD & Assistant Professor, NIMS School of Law, NIMS University Rajasthan, Jaipur

(Received: 16 March 2025

Revised: 20 April 2025

Accepted: 01 May 2025)

KEYWORDS

Deepfake, manipulation, misinformation, influence, cyber frauds.

ABSTRACT:

With the ongoing trends and development of Artificial Intelligence there has been the emergence of deepfake technology. This technology manipulates the audio and visuals of an original content to create a new one which is synthesized and manipulated. In the recent times the internet specially the social media are full of such deepfake videos which on one hand is violating the privacy of an individual or personal rights of a celebrity and on the other hand are misleading the viewers. In addition, various incidents of cyber frauds are being reported which are committed using this deepfake technology. This paper deals with the concept of deepfake and certain technical aspects that are involved in their creation. Along with this, the paper is focused on highlights Indian and international instances of deepfakes which were misleading and made use of various celebrities and politicians. In addition, the paper highlights comparative study of the Indian laws and the U.S. based laws that deal with the deepfake content with special reference to the Information Technology Act, 2000 and the Bhartiya Nyaya Sanhita, 2023, Malicious Deep Fake Prohibition Act of 2018 and DEEP FAKES Accountability Act. Lastly the paper mentions the impact of spread of deepfake videos on social media platforms and measures to deal with it.

Objective- The paper aims to highlight the different aspects of deepfake videos with reference to its impact and the laws dealing with it.

1. Introduction

Living in the time where the AI is still regarded as in its developing phase, yet we have reached the stage where the use of AI related technology is affecting our lives. One of such uses of the AI is the creation of deepfake content in which the software's make use of deep learning algorithms and create a manipulated digital media content which appears to be highly realistic. The term 'deepfake' was coined by a Reddit user in 2018. The deepfakes appear to be so genuine that it is challenging for people even to decipher whether it is original or manipulated audio or visual. Even the individual's whose voice, images, or videos are used from the original source and then manipulated to create a deepfake it is difficult to decipher that the deepfake which is making use of the person.

What is Deepfake- Deepfake refers to an artificial video or a series of images which is generated by the use of machine learning. A special type of machine learning called as 'deep learning' is being used to generate the same. Deep learning is a special machine learning wherein an algorithm is put forward involving the use of a real video or image of an individual which is further processed and to create an output that resembles the original content.

Technical aspect and development of a deepfake- In order to create a deep fake content, 'hidden layers' are used. The further execution involves an algorithm known as 'neural network', which replicates the original learning way of a human being. In a 'hidden layer' series of nodes perform mathematical transformations that convert input signals to output signals like converting a real content to an unrecognizable fake content. The extensively hidden deeper neural network performs its task on the real content for creating a recursive neural



network (RNN) which simply means image recognizing and applying it to create deep fake video.

Deep fake involves the use of 2 algorithms. The initial one is trained with producing best replicas of real image and the later one is trained with the detection of a fake and real video or image. These 2 algorithms work in coordination with each other and put forward a model that is capable of producing fake videos or images. This fake or replicated creation is generally not recognized by people as a fake one.

2. Circulation of Deepfakes

Over the past years the internet has been flooded with the numerous deepfake videos. As per the reports of Deep Media¹, in 2023 around 500,000 audio a video deepfake circulated on the social medias. It is roughly estimated that by 2025, the number of such videos is expected to rise up to 8 million videos.

Social media platforms are such platforms from where the circulation of the information takes place in a fast pace and the outreaches to millions of people at a single click. This potential of social media has become a bait to widespread of deepfake that continue to spread misinformation and mislead people.

In addition, with the use of social media platforms the deepfake have developed a negative trend by using the faces or voice overs of the celebrities be it known movie actors, or singers or journalists or industrialists or politicians.

Deepfake are unhesitatingly making use of their visuals or audios to mislead common individuals and go on committing various sorts of financial scams, frauds or cybercrimes.

The social media platforms have witnessed various such instances wherein popular celebrities became a tool of deepfake. Some of these instances can be studied from 2 perspectives, namely:

- Indian instances of deepfake and
- International instances of deepfake

Indian Instances of deepfake

In December 2023, Ratan Tata (ex-chairman of Tata Group) came out exposing a deepfake wherein it was showcased that he was giving some financial and investment advices which are risk free.

Narayana Murthy, the founder of Infosys, also highlighted the existence of several deepfake videos circulating on the internet featuring him.

"In recent months, there have been several fake news items propagated via social media apps and on various webpages available on the internet claiming that I have endorsed or invested in automated trading applications," Murthy wrote on the microblogging site.

Priyanka Chopra, the actress deepfake circulated where she was spotted endorsing a brand in a misleading video. Similarly, actress Alia Bhatt was featured in a deceptive deepfake video showing her face digitally placed onto another woman, depicted sitting on a bed. Another most controversial instance where Rashmika Mandanna, the actress's face was used in deepfake of her being in an explicit situation. In her comments on X, Mandana wrote, "I feel really hurt to share this and have to talk about the deepfake video of me being spread online. Something like this is honestly, extremely scary not only for me, but also for each one of us who today is vulnerable to so much harm because of how technology is being misused."

The famous cricketer Sachin Tendulkar also could not escape such circulation of a deepfake of his. He reported on his social media account of a deepfake video of him promoting a certain mobile application. He further expressed his dismay at the widespread misuse of technology. "These videos are fake. It is disturbing to see rampant misuse of technology. Request everyone to report videos, ads & apps like these in large numbers. Social Media platforms need to be alert and responsive to complaints. Swift action from their end is crucial to stopping the spread of misinformation and deepfakes," Sachin Tendulkar said in a post on X.²

¹ Alexandra Ulmer and Anna Tong, 'Deep faking it: America's 2024 election collides with AI boom' (*Reuters*, May 31, 2023) <<https://www.reuters.com/world/us/deepfaking->

[it-america-2024-election-collides-with-ai-boom-2023-05-30/](https://www.reuters.com/world/us/deepfaking-america-2024-election-collides-with-ai-boom-2023-05-30/) > accessed 22 March 2025

² Sangeets Ojha, 'From Ratan Tata, Sachin Tendulkar to Madhusudan Kela: 9 well-known personalities who were victims of deepfake videos' (*Mint*, 14 March



International instances of deepfake

In April 2018, a Deepfake of Barack Obama was created by comedian Jordan Peele in collaboration with BuzzFeed which served as a public service announcement (PSA) to increase awareness of Deepfakes³

Another instance showcased that during the Christmas holidays; Queen Elizabeth II was shown dancing across TV screens as part of a British broadcaster's warning against the proliferation of misinformation⁴

In June 2019, a controversial deepfake video of Malaysia's Economic Affairs Minister circulated depicting him being involved in a physical relation.⁵

In 2020, Extinction Rebellion Belgium released a fabricated video of then Belgian prime minister Sophie Wilmes appearing to connect the spread of COVID-19 to uncontrolled ecological crises. The video made use of her original address to the people during the pandemic and then developed a fake one with some another script.⁶

During March 2022, a deep fake of the President of Ukraine Volodymyr Zelenskyy circulated of him urging the military to put down their weapons and surrender. This was amid the ongoing war between Russia and Ukraine. Taking into consideration the critical was situations the President's office held no delay and denied the video as unauthentic and was generated by making use of the deepfake technology.⁷

Another dark side of the deepfake videos emerged when the sexually explicit pictures of the famous singer Taylor Swift. The famous actress knows for the role of 'Wonder Woman' became the victim of a deepfake where her face was used in a pornographic film.⁸

*"Deepfake technology is being weaponized against women by inserting their faces into porn. It is terrifying, embarrassing, demeaning, and silencing. Deepfake sex videos say to individuals that their bodies are not their own and can make it difficult to stay online, get or keep a job, and feel safe."*⁹

To add up these instances, another deepfake circulated of Steve Harvey where he was showed in promoting a government fund, while on the contrary it was a scam.

3. Existing Laws in India

There is no particular law in India that specifically counters the use and spread of AI generated deepfakes. However, within the purview of existing laws the deepfake content can be dealt. These provisions are:

- The supreme court of India has regarded the right to privacy as a fundamental right under Article 21 of the Constitution of India.¹⁰
- Section 66 of THE INFORMATION TECHNOLOGY ACT, 2000- wherein "any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for

2024) <<https://www.livemint.com/news/india/from-ratan-tata-sachin-tendulkar-to-madusudan-kela-9-well-known-personalities-who-were-victims-of-deepfake-videos-11710307982420.html>> accessed 18 March 2025

³ Craig Silverman, 'How to Spot a Deepfake Like the Barack Obama-Jordan Peele Video' (*Buzzfeed*, 17 April 2018) <<https://www.buzzfeed.com/craigsilverman/obama-jordan-peeel-deepfake-video-debunk-buzzfeed>> accessed 18 March 2025

⁴ Zamira Rahim, "'Deepfake' Queen delivers alternative Christmas speech, in warning about misinformation" (*CNN World* 25 December 2020) <<https://edition.cnn.com/2020/12/25/uk/deepfake-queen-speech-christmas-intl-gbr>> accessed 22 March 2025

⁵ Northwestern University Buffett Institute for global affairs, 'The Rise of Artificial Intelligence and Deepfakes' (2023) <https://buffett.northwestern.edu/documents/buffett-brief_the-rise-of-ai-and-deepfake-technology.pdf> accessed 21 March 2025

⁶ Id.

⁷ Id.

⁸ Samantha Cole, 'AI-Assisted Fake Porn Is Here and We're All Fucked' (*Vice*, 11 December 2017) <<https://www.vice.com/en/article/gal-gadot-fake-ai-porn/>> accessed 21 March 2025

⁹ Danielle Citron, Professor of Law, Boston University, and author of *Hate Crimes in Cyberspace*, <https://www.hup.harvard.edu/books/9780674659902>

¹⁰ *Justice K.S. Puttaswamy (Retd) And Anr. vs Union of India and Ors.* [2017] AIR 2017 SUPREME COURT 4161



a term which may extend to three years or with fine which may extend to five lakh rupees or with both.”¹¹

- Section 43 of The Information Technology Act, 2000 provides with the penalty and compensation for the damage caused to the computer or computer system.

As per this provision if a person gains access, downloads or copies data, introduces a virus in the computer, disrupts or denies access to the authorized person, or alters, steals conceal any data without the permission of the owner of a computer, then such person shall be liable to pay compensation to such owner.¹²

- Section 66E of the Information Technology Act, 2000 provides with the punishment for the violation of privacy. As per this provision, the intentional capturing, publishing or transmission of a private area of a person, without his consent, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.¹³

- Section 79 (3) of the Information Technology Act, 2000 makes an intermediary liable if such intermediary has conspired, abetted, aided the commission of an unlawful act, or on his failure to remove or disable the access to such unlawful act, on being notified by the appropriate Government.¹⁴

- Section 356 of the Bhartiya Nyaya Sanhita, 2023 provides with the defamation wherein publication by words spoken or intended to be read or by signs, visible representations that harms the reputation of a person, is said to defame that person.¹⁵

4. Guidelines by Ministry of Electronics and Information Technology (MeitY)

Ministry of Electronics and Information Technology (MeitY) has issued directives specifically targeting the growing concerns around misinformation powered by AI – Deepfakes.

The advisory stated that, “The content not permitted under the IT Rules, in particular those listed under Rule 3(1)(b) must be clearly communicated to the users in clear and precise language including through its terms of

service and user agreements and the same must be expressly informed to the user at the time of first-registration and also as regular reminders, in particular, at every instance of login and while uploading/sharing information onto the platform.”¹⁶

The advisory emphasizes that digital intermediaries must ensure users are informed about penal provisions, including those in the IPC and the IT Act 2000, in case of Rule 3(1)(b) violations.¹⁷

“The users must be made aware of the various penal provisions of the Indian Penal Code (IPC) 1860, the IT Act, 2000 and such other laws that may be attracted in case of violation of Rule 3(1)(b). In addition, the terms of service and user agreements must clearly highlight that intermediaries/platforms are under obligation to report legal violations to the law enforcement agencies under the relevant Indian laws applicable to the context,” the advisory further added.¹⁸

Rule 3(1)(b) within the due diligence section of the IT rules mandates intermediaries to communicate their rules, regulations, privacy policy, and user agreement in the user’s preferred language. They are also obliged to ensure reasonable efforts to prevent users from hosting, displaying, uploading, modifying, publishing, transmitting, storing, updating, or sharing any information related to the 11 listed user harms or content prohibited on digital intermediaries. This rule aims to ensure platforms identify and promptly remove misinformation, false or misleading content, and material impersonating others, including deepfakes.¹⁹

Minister Shri Rajeev Chandrasekhar stated, “Misinformation represents a deep threat to the safety and trust of users on the Internet. Deepfake which is misinformation powered by AI, further amplifies the threat to safety and trust of our Digital Nagarik’s. On 17th November, the Prime Minister Shri Narendra Modi alerted the country to the dangers of deepfakes and post that, the Ministry has had two Digital India Dialogues

¹¹ The Information Technology Act 2000, s 66

¹² The Information Technology Act 2000, s 43

¹³ The Information Technology Act 2000, s 66E

¹⁴ The Information Technology Act 2000, s 79(3)

¹⁵ The Bhartiya Nyaya Sanhita 2023, s 356

¹⁶ Ministry of Electronics & IT, *MeitY issues advisory to all intermediaries to comply with existing IT rules*

(2023)

<
<https://pib.gov.in/PressReleaseIframePage.aspx?PRID=1990542>> accessed 22 March 2025

¹⁷ Id.

¹⁸ Id

¹⁹ Id



with all the stakeholders of the Indian Internet to alert them about the provisions of the IT Rules notified in October 2022, and amended in April 2023 that lays out 11 specific prohibited types of content on all social media intermediaries & platforms.”²⁰

The Minister further emphasized that Rule 3(1)(b)(v) explicitly prohibits the dissemination of misinformation. Consequently, all intermediaries were asked to exercise due diligence in promptly removing such content from their platforms. He also emphasized that platforms have been duly informed about the legal consequences associated with any violations under the IT rules.²¹

“Rule 3(1)(b)(v) prohibits misinformation and patently false information. During the two Digital India Dialogues, Government and industry have agreed to more measures to ensure compliance by platforms and users with the IT rules which have been explained earlier in the media. Today, a formal advisory has been issued incorporating the ‘agreed to’ procedures to ensure that users on these platforms do not violate the prohibited content in Rule 3(1)(b) and if such legal violations are noted or reported then the consequences under law will follow. MeitY will closely observe the compliance of intermediaries in the coming weeks and follow this up with further amendments to the IT Rules and/or the law if and when required. It is Prime Minister Shri Narendra Modi government’s mission to ensure that the internet is safe & trusted and all intermediaries are accountable under law for the safety and trust of the Digital Nagarik’s that use the Indian Internet,” the Minister further added.²²

5. Laws in USA

Malicious Deep Fake Prohibition Act of 2018

The bill was introduced in the 115th CONGRESS 2d Session to amend title 18 of the United States Code in order to prohibit the fraudulent audiovisual records, and for other purposes.

SEC. 2. Fraud in connection with audiovisual records

§ 1041. Fraud in connection with audiovisual records

The section specifically defines the term ‘deep fake’ as “audiovisual record created or altered in a manner that the record would falsely appear to a reasonable observer to be an authentic record of the actual speech or conduct of an individual”²³

Further it shall be unlawful to use any means or facility of the interstate or foreign commerce to create with the intent to distribute a deepfake.²⁴

The penalty for the above offence shall be- “fined under this title, imprisoned for not more than 2 years, or both; or

“(2) fined under this title, imprisoned for not more than 10 years, or both, in the case of a violation in which the creation, reproduction, or distribution of the deep fake could be reasonably expected to—

“(A) affect the conduct of any administrative, legislative, or judicial proceeding of a Federal, State, local, or Tribal government agency, including the administration of an election or the conduct of foreign relations; or

“(B) facilitate violence.”²⁵

“Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2023” or the “DEEP FAKES Accountability Act”

Object- The Act aims to protect national security against the threats posed by deepfake technology and to provide legal recourse to victims of harmful deepfakes.

The Act defines ‘advanced technological false personation record’ as any deepfake which makes a reasonable person to believe that the visual or audio quality of the record exhibits any material activity of living or deceased person and such record was produced without the consent of such living or heirs of the deceased person.²⁶

²⁰ Id

²¹ Id

²² Id

²³ Malicious Deep Fake Prohibition Act of 2018, s 3805 § 1041(a) (2)

²⁴ Malicious Deep Fake Prohibition Act of 2018, s 3805 § 1041(b)(1)– (2)

²⁵ Malicious Deep Fake Prohibition Act of 2018, s 3805 § 1041(c)(1)– (2)

²⁶ Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to



Also defines ‘online platform’²⁷ in order to implement certain rules on such platforms. In addition, the Act provides with deepfake victims assistance.²⁸

It also focuses on the detection of task force by establishing of a “deep fake task force” in Department of Homeland Security and by private sector collaboration in order to research and develop technologies to detect and combat deepfake and other types of advanced image manipulation.²⁹

The Act also focuses on the need for information sharing between the online platform and the Department of Homeland Security for the prompt alertness dissemination of deepfake.³⁰ In addition it is compulsory for the online platforms to have a system to detect deepfake and technical advancement and capability to disclose the origin of the deepfake which was distributed on their platform.³¹

The act also provides with penalty in form of- criminal, civil, private right of action, injunction, damages.³²

SEC. 5709. Report on Deepfake Technology, Foreign Weaponization of Deepfakes, And Related Notifications

The Direct of National Intelligence shall be submitted with a report on the potential national security impact of machine manipulated media (‘deepfake’) and the actual or potential use of machine manipulated media.³³

Accountability Act of 2023 H. R. 5586, § 1041 S. 2 (n) (1) (A)-(B)

²⁷ Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2023 H. R. 5586, s 10 (d) (2)

²⁸ Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2023 H. R. 5586, § 1042.

²⁹ Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2023 H. R. 5586, s 7 (a)-(b).

³⁰ Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2023 H. R. 5586, s 9

³¹ Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2023 H. R. 5586, s 10

³² Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to

Laws developed by other nations

In addition, the States legislatures are also proposing measures to counter the spread of deepfakes like Virginia³⁴, Texas³⁵ and California³⁶. Following the same China³⁷ has also criminalized the publication of deepfake without adequate disclosure.

6. Impact of Deepfake on society

The ambit of deepfake hints of not slowing down and now involves common individuals as well. The common people are becoming subject to various cyber frauds.

Spread of misinformation- The spreading of false information could lead to panic, hatred and violence which could further lead to unrest between the communities and society.

Political influence- Deepfake bear the potential to hamper the democratic processes like elections by spreading out misinformation about the candidates, leaders and policies.

Cyber threats and privacy violations- The deepfake pose the potential to personate an individual which could further lead unauthorized access to personal and confidential data.

In addition to this, a common individual becomes prone to cyber fraud through such impersonation. For instance, the first deepfake fraud was reported in Kerala in July 2022. Herein a Radhakrishnan, 73-year-old man received a video call from a person who was his former colleague,

Accountability Act of 2023 H. R. 5586, s 2 § 1041 (f) (1)-(2), (g) (2)-(3)

³³ Report on Deepfake Technology, Foreign Weaponization of Deepfakes, And Related Notifications s 5709

³⁴ Adi Robertson, ‘Virginia’s ‘revenge porn’ laws now officially cover deepfakes’ (The Verge, 2 July 2019) <<https://www.theverge.com/2019/7/1/20677800/virginia-revenge-porn-deepfakes-nonconsensual-photos-videos-ban-goes-into-effect>> accessed 20 March 2025

³⁵ Texas Senate Bill number 751 2019

³⁶ California Assembly Bill number 730 2019

³⁷ Nick Statt, ‘China makes it a criminal offense to publish deepfakes or fake news without disclosure’ (The Verge, 2019) <<https://www.theverge.com/2019/11/29/20988363/china-deepfakes-ban-internet-rules-fake-news-disclosure-virtual-reality>> accessed 19 March 2025



named Vennu Kumar. The call made use of the deepfake technology in which the voice and appearance of Vennu Kumar. The person posing as Vennu Kumar requested for a loan of Rs. 40,000 from Radhakrishnan as he was in a crisis and urgently needed money. Having prior acquaintances, Radhakrishnan immediately transferred money. However, the instance got reported and during the investigation it was found that it was a deepfake call which made use of fraudster sophisticated AI software. In addition, the personal information about Radhakrishnan was obtained from the social media account of his friend VennU Kumar.³⁸

This instance reflects the potential threat of AI generated deepfake and in such a case there are 2 victims, one against whom the financial fraud was committed and second whose social media handle was infiltrated and personal data was obtained thus, leading to his breach of privacy.

7. Measures to overcome

New regulatory measures- The current IT Act, 2000 and the criminal laws are not sufficient to specifically deal with the growing threats due to deepfake. The Ministry of Electronics and Information Technology (MeitY) has issued certain guidelines with respect to the same however in the upcoming time where the development, reach and threat of the deepfake technology would continue to rise, it becomes essential to develop certain key focused laws with respect to the use of deepfake or to amend the existing laws keeping intact the focus again on the regulatory measures to counter the threat posed by the deepfake.

In addition, it becomes essential to create a separate wing in the administrative units like cyber team that lay their focus on detection of such deepfake that pose the threat to the society and bear the potential to cause cyber frauds or unrest in the society.

Technological advancement- Undoubtedly, it becomes necessary for the development of new software's that are equipped enough to deal with 3 major aspects like-detection the deepfake videos, deciphering the source of such videos, instant removal of such videos from social

media platforms, in order to minimize its impact on the people.

In addition, it becomes essential that such technology is put to use in the courts which would aid the Court and judges to deal with the cases of deepfake smoothly.

For instance, in the case of *Nirmaan Malhotra vs Tushita Kaul*³⁹, the Delhi High Court in this application for maintenance to wife emphasized on the possibility of the use of deepfake images against the accusation of adultery and hence the maintenance for granted for the time being. The Court stated- "We have looked at the photographs. It is not clear as to whether the respondent/wife is the person in the photographs, as alluded to by the learned counsel for the appellant/husband. We may take judicial notice of the fact that we are living in the era of deepfakes and, therefore, this is an aspect that the appellant/husband, perhaps, would have to prove by way of evidence before the Family Court."

Therefore, in cases that involve the use deepfake, it is essential that the Courts are technically equipped to deal with such deepfake cases.

Duty of social media platforms- the Government can share the technology with the social media platforms in order to detect and minimize the risk posed by a deepfake content. In addition, such platforms could be imposed with the duty to detect the source of such deepfake content or to remove such content as soon as it is revealed that the content circulating is made out of deepfake technology.

Media literacy- the journalists play a crucial role in making common people aware about the concept of deepfake videos, the misinformation spread through them and the cyber frauds committed through use of such technology.

For instance, the popular journalist Rajat Sharma on his show clearly mentioned about the circulation of a deepfake video of his own. He took continuous awareness measure to aware people about the misinformation spread by such deepfake videos and the cyber frauds committed with their help.

³⁸ Indian Cyber Squad, *Case Study: Kerala's First Deepfake Fraud*
<<https://www.indiancybersquad.org/post/case-study-kerala-s-first-deepfake-fraud>> 18 March 2025

³⁹ *Nirmaan Malhotra vs Tushita Kaul* [2024] MAT.APP. (F.C.) 180/2024 &CM Nos.32316-18/2024



Setting industry standards- in case of the use of deepfakes which is purely generated for entertainment purpose, it should be made necessary for the platform making and using it to provide disclaimers about such deepfake generated content.

8. Conclusion

We are living in era where every individual be of any age group is equipped with the smart phones and access to available internet. This combination of technology is indeed a boon for various reasons like global connectivity, resource sharing, trade, healthcare, education etc. However, with the tremendous increase of use of internet there has been a rise in evolution of various social media platform which initially were meant to connect globally and entertainment purpose, has now become prone to the spread of misinformation that can further lead to unrest in the society and to commit cyber frauds.

One of such key features is the use of deepfake which initially used for entertainment purpose had now come down to spread misinformation by use of popular faces who have their vast reach among the masses. Deepfakes of such popular celebrities are circulating on that near the potential to commit cyber frauds. In addition, to the victim of such misinformation it is the celebrities who are aggrieved of identity theft and misuse of their personal right, which have been recognized by the Supreme Court of India on various occasions like in the cases of Rajnikanth⁴⁰, Amitabh Bachchan⁴¹ and Anil Kapoor.⁴² Apart from the deepfakes of celebrities, common individuals are also becoming the faces of such videos which are further used to generate explicit content related to pornography, especially women are becoming prey of such content and in the upcoming times such crime against women also needs to dealt with.

Therefore, it becomes the need to counter this misuse of technology and bring in some profound laws that counter crimes that are now transformed and committed by use of AI and technology.

As previously discussed, Indian technology related laws require a new aspect that concentrates specifically on the development, spread of deepfakes and fast response to stop such circulation. In addition, the execution of such laws requires a separate panel of IT experts who behold a quick response to handle the spread of such misinformation through deepfake videos.

⁴⁰ *Shivaji Rao Gaikwad vs. Varsha Productions* [2015] Civil Suit No.598 of 2014

⁴¹ *Amitabh Bachchan vs Rajat Nagi & Ors* [2022] CS(COMM) 819/2022

⁴² The Hindu Bureau, 'Can't misuse Anil Kapoor's persona, catchphrase 'jhakhaas', HC says *The Hindu*

(New Delhi, 24 September 2023)

<<https://www.thehindu.com/news/cities/Delhi/cant-misuse-anil-kapoors-persona-catchphrase-jhakhaas-hc-says/article67326277.ece>> accessed 17 March 2025