© MAY 2026 | IRE Journals | Volume 9 Issue 11 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I11-1717796

Legal Protection against Non-Consensual Deepfake Content in India

DIVIKA UPPAL
Amity Law School, Noida

Abstract- ***This dissertation focuses on the newly emerged phenomenon of deepfakes and its intricate legal aspects, analyzing it mostly through the Indian legal system and a comparative perspective of how the legal systems of different countries operate. Deepfakes are generated with the help of the latest artificial intelligence methods, including Generative Adversarial Networks (GANs), and allow producing highly realistic and fake audio-visual content, which is associated with grave concerns regarding privacy, reputational concerns, misinformation, and democratic integrity. The paper starts by discussing the conceptual and technological background of deepfakes, their development and the different types and uses of them in entertainment, politics, and cybercrime. It also harshly evaluates the dangers of deepfakes, such as identity theft, defamation, non-consensual explicit content, and mass-disinformation campaigns. The study also assesses the moral issues and social implications of the abuse of such technology. The dissertation dedicates a considerable portion to the analysis of the sufficiency of the current Indian legislation such as the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Digital Personal Data Protection Act, 2023, to deal with harms caused by deepfakes. It further takes into account intermediary liability in the context of the Information Technology Rules, 2021, and examines the judicial cases that influence the discussion of the privacy and free speech in the digital era. The paper singles out regulatory issues including lack of specific legislation on deepfakes, technological constraints in the detection process, jurisdictional issues, and the conflict between freedom of speech and regulation. In order to give a broader picture, a comparative review of the legal systems in other countries like the United States, European Union and the United Kingdom is also conducted with a focus on best practice and trends in regulation. The dissertation ends by suggesting legal and policy recommendations such as the necessity of specialized legal framework, greater platform responsibility, enhancing technological detection systems, and global collaboration. It stresses the need to adopt a balanced strategy that does not only protect basic rights but also effectively deals with the menace of deepfake technology in an ever-digitalized society.***

Keywords: Deepfakes, Artificial Intelligence, Generative Adversarial Networks (GANs), Cybercrime, Identity Theft, Defamation, Misinformation, Digital Privacy, Intermediary Liability, Information Technology Act, 2000 Information Technology Act, 2000, Digital Personal Data Protection Act, 2023 Digital Personal Data Protection Act, 2023, Bharatiya Nyaya Sanhita, 2023 Bharatiya Nyaya Sanhita, 2023

I. INTRODUCTION

Meaning and Concept of Deepfakes

Deepfake has become one of the most important technological and legal issues of digital times. Deepfakes are a term based on the combination of deep learning and fake, where synthetically produced media content relies on the advanced artificial intelligence (AI) algorithms to produce extremely realistic yet false images, events, or speech. These technologies are based more on machine learning models, specifically Generative Adversarial Networks (GANs), which work by pitting two neural networks against one another, where the former creates synthesized content, and the latter judges it to be real or not, until the former is almost indistinguishable to real data.

Deepfake technology is a significant advancement over previous digital editing technologies like photo editing or video splicing. Conventional methods of editing demanded quite a lot of technical knowledge and would frequently leave the traces. Deepfakes, in turn, can create continuous and very believable results, which is much harder to detect. As the user-friendly software and mobile applications spread, the design of deepfakes is becoming more accessible, decreasing the entry barrier, and allowing its usage in many industries.

The idea of deepfakes is a threat to the basis of evidentiary reliability in the digital age. Traditionally,

visual and audio records have been considered as valid types of evidence both in legal and social settings. Nonetheless, with the advent of deepfakes, there is a new degree of uncertainty that is compromising this assumption. This power to create realistic material, casts serious doubts on authenticity, trust and integrity of the information.

In terms of functionality, deepfakes can be divided into a number of types, such as:
Face-swapping videos, in which the face of one person is overlaid on the body of another.
Voice synthesis, imitating the speech of a person, his/her tone.

- Lip-sync, audio is altered to fit modified video material.
- Full-body synthesis, that synthesizes complete visual representations.

Although deepfakes can be used legitimately to benefit the entertainment industry, education, and accessibility, their abuse is a grave legal and ethical issue. To illustrate, deepfakes can be applied in the entertainment sector to re-create past events or improve movie experience. They can be used to enable immersive learning in the educational field. The risks of malicious use, however, dwarf these advantages.

Evolution of Deepfake technology
It can be traced back to the year 1960s.
Deepfake technology is directly connected with the progress in artificial intelligence and machine learning. Deepfake-like techniques can be traced to the early works of computer vision and image processing, where digital images and videos were manipulated by using algorithms. But such early techniques had shortcomings, they yielded unrealistic results.

The deep learning, which is a subset of machine learning, was the turning point in the evolution of deepfake technology, as it involves using a neural network consisting of multiple layers, analyzing it to produce complex patterns and generating complex data. The development of the Generative Adversarial Networks (GANs) in 2014 was a breakthrough as it made it possible to create very realistic synthetic media. Deepfake is a commonly used term that started gaining popularity around 2017 when people started using AI-assisted tools in order to generate manipulated videos, especially those of celebrities. All these early applications demonstrated the potential of the technology but also its potential to be abused.

Since, the deepfake technology has been taking an unprecedented turn of development, courtesy of the increased power of computing, accessibility of large data sets, and the development of better algorithm design. Deepfakes can be created with a comparatively simple technology, such as smartphone applications, today, which makes the technology accessible to a wide audience.

Importance of the research.
The importance of the work is that it addresses one of the rapidly developing issues that have far-reaching consequences in the legal, social, and governance spheres. Deepfakes are a special dilemma since they are a combination of cybercrime, privacy invasion, misinformation, and technology advancements.The influence of deepfakes on the rights of individuals, especially the right to privacy and reputation is one of the main motivating factors to study it. The illegal use of image or voice of an individual may lead to a lot of harm such as emotional distress, tarnished reputation and societal stigmatization.

Research Objectives
The main aim of this dissertation is to critically analyze how deepfakes can and are regulated under Indian law as well as to assess the effectiveness of the current laws in combating the challenges brought about by this technology.

The study objectives will be:
1. To examine the idea and technology behind deepfakes, how they are formed, their kinds, and uses.
2. To discuss the legal framework of deepfakes in India, specifically, the IT Act and the laws related to deepfakes, including the BNS.
3. To find out the weaknesses and shortcomings of the current legislation in combating deepfake-related crimes.
4. To perform a comparative study on the regulatory approaches in the jurisdictions like the United States, the United Kingdom and the European Union.

Scope and Limitations of the Study
Scope of the Study
This dissertation is both analytical and comparative since it examines the role of regulating deepfakes in the Indian legal system, as well as using the insights of other jurisdictions.

The focus of the study is mainly:
The idea and technology behind deepfakes.

- Legal requirements in the IT Act, BNS and other laws.
- The importance of intermediary regulations, specifically, Information Technology (Intermediary Guidelines and Digital Media Ethics Code), 2021.

Obstacles to privacy and freedom of expression as per the constitution.

- Court action and case law (where relevant)

Comparison with other chosen jurisdictions.
The study is doctrinal in nature and it dwells on the statutory interpretation and judicial rulings and principles of law. It also uses some aspects of the policy analysis to determine how effective the current structures are.

Strengths of the Study.
The study has some limitations although they are not in the scope of the study:
1.Lack of Specific Legislation on Deepfakes in India: Lack of specific legislation that is designated to deal with deepfakes is one of the main problems. Consequently, the research is based on the interpretation of the existing laws, which might not be able to reflect all the aspects of the problem.
2. Blistering Technological Change Deepfake: technology is changing fast, and in most cases; it is ahead of the creation of laws. This poses a threat whereby some of the analysis aspects might become obsolete due to the ever-growing technology.

II. RESEARCH METHODOLOGY

The approach taken in this dissertation is mainly doctrinal and analytical with some elements of the comparative and descriptive approaches. This approach is suitable because of the legal subject of the study and the emphasis on the interpretation of the statutes and consideration of the policy.
1. Doctrinal Research
The study relies on the main part of the research which is the doctrinal research i.e. the analysis of the legal texts and includes:
Statutes e.g. IT Act and BNS.
Rules and regulations (intermediary guidelines).
Judgment and case law.
Commentaries on the law and scholarly articles.
This method will allow performing a systematic study of the legal framework of deepfakes.

2. Analytical Method
This paper uses an analytical approach in critically assessing the effectiveness of the laws in place. This involves:

- Determining weaknesses and inconsistencies in the law.
- Evaluation of sufficiency of existing provisions.

E- Study of the practical difficulties of enforcement.
The method of analysis enables one to have a greater insight into the strengths and weaknesses of the law.

3. Comparative Method
An analysis is conducted on how the issue of deepfakes has been dealt with in other jurisdictions. This includes:

- the study of the legislative systems in the USA, UK and European Union.
- Finding most effective practices and new regulation strategies.
- The assessments of applicability of these methods to the Indian context.

The comparative approach offers a lot of insight and assists in guiding the reform recommendations.

This chapter discusses the current legal provisions which apply to deepfakes such as the IT Act, BNS and intermediary provisions.

Understanding Deepfakes and Their Legal Implications
Technical overview of the Deepfake Technology.
This paper will begin by first providing an introduction into the Deepfake Technology.

The Deepfake is a more sophisticated type of synthetic media, which is created based on the methods of Artificial Intelligence. It is mainly based on the subfields of Machine Learning and Deep Learning to produce highly realistic, yet man-made audio-visual data. The name deepfake is a combination of deep learning and fake, as the process is based on the former and the result is misleading.

In contrast to conventional digital editing techniques where people have to manually manipulate their data and it can be easily traced in most cases, deepfake technology utilises automated learning algorithms which process large amounts of data, be it images, videos or audio samples. Patterns that include facial expressions, speech rhythms and behavioral features are learnt by these systems and therefore they can imitate human beings in an incredible manner.

Deepfakes: types and usages.
(a) Face-Swapping Deepfakess
This is the most widespread type of deepfake where an individual face is overlaid on to the bodies of another in a video or image. It uses deep learning models that are trained with the use of facial datasets to mimic facial expressions and movements.
(b) Voice cloning (Audio Deepfakes)
Voice cloning is the production of fake speech which resembles a certain person. Through tone analysis (voice samples), AI can recreate tone, pitch and speaking style.
(c) Lip-Sync Deepfakes
This is in the form of changing the lip movements of an individual in a video to fit in the fake audio. The rest of the facial features are not affected as is the case with face-swapping.

3. Intent/Use Classification.
Deepfakes also may be classified according to their purpose:
There are legitimate and beneficial uses of this (A) above.
-Entertainment Industry
Visual effects, such as de-aging actors, dubbing and recreation of historical figures, are created with deepfakes.
-Education and Training
They allow interactive learning, e.g. historical simulation and language training.
-Accessibility
The voice cloning technology helps those who have indiv iduous speech and can enable them to communicate.
-Marketing and Advertising
The personalised advertisements and online campaigns are done using AI-created content.

Viruses and other malicious and harmful applications.
1. Non-Consensual Explicit Content
Deepfakes are highly abused to generate explicit content with no permission and cause dire privacy invasion.
2. Fake News and Political Interference.
There is a risk of fake videos of public officials deceiving the masses and destabilising democracy.
3. Fraud and Cybercrime
Financial frauds, phishing and identity thefts are performed through voice cloning and video impersonation.

Statutory Framework
There is no particular law on deepfaking in India. Rather, several laws, which can be considered together, deal with various elements of harm, which deepfakes cause:
* Cyber Laws: The Information Technology Act, 2000, is the law which governs cyber law.
Criminal Law: This has now been regulated by Bharatiya Nyaya Sanhita, 2023.
Data Protection: Falling under the Digital Personal Data Protection Act, 2023.
Intermediary Regulations: of the Information technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
All of these laws deal with a particular aspect of the harm related to deepfakes, including identity theft, obscenity, or privacy invasion or intermediary liability.

Absence of Specific Legislation on Deepfakes
In India, a specific statutory framework does not exist, which can be seen as one of the key impediments to the regulation of deepfakes. Deepfake technology is a new type of digital manipulation based on artificial intelligence, but the Indian law has not kept pace with the new technology to deal with its peculiarities. Legal reactions, therefore, are mostly based on the already existing laws which were not intended to govern the

synthetic media and create uncertainty in interpretation and enforcement.

Problems with Detection and Attribution.
1. Generating Deepfakes is Technically Complex.
Deepfakes are made by the use of sophisticated artificial intelligence (AI), in the form of deep learning models and neural networks.
2. Weaknesses of Detection Technologies.
Despite the development of a variety of different detection tools, they have certain limitations:
False Positives and Negatives: Authentic content can be detected as a fake one, whereas advanced deepfakes can be left unnoticed.
3. Attribution and Anonymity Problems.
One of the most challenging areas of regulation is to attribute deepfake material to a particular person. Key challenges include:
Anonymity and Pseudonymity: False identities can be used by the users.
Use of VPNs and Encryption: these are used to mask the source of content.
4.Effect on Law enforcement agencies.
There are various operational challenges that law enforcement agencies have to deal with:
Poor technical skills on AI and digital forensics.
Unavailability of state-of-the-art detection equipment.

Key principles include:
Legal Processing of Personal Data.
Consent Requirements
Purpose Limitation and Minimization of Data.
Data Subjects (access, erasure, etc.) Rights.
Deepfakes frequently entail the use of personal information without the relevant permission, thus, breaking these principles. The victims can use the data protection law to remedy any abuse of their personal data.

Conclusion and Recommendations
The research notes that although India has a legal framework on which to build upon, it is not comprehensive enough to deal with the intricacies of deepfake technology. It is necessary to have a very clear, coordinated and future-oriented approach to regulations.
the deepfake regulation needs a multi-layered and complex approach that incorporates legal, technological, and institutional regulation. The present structure of India requires reforms in order to effectively deal with these complexities.

Deepfakes must be regulated in a holistic and proactive manner, which involves changes to the laws, technological development, and international collaboration. Through these suggestions, India will be able to build a solid regulatory framework that can effectively deal with human challenges of the deepfake technology and protect fundamental rights and innovations.

Policy interventions cannot be done without technology in controlling deepfakes. Technological tools and policy measures allow proactive and effective enforcement, although a legal framework is the basis to do so. There should be a coordinated effort to counter the threats of deepfake technology through a concerted effort of all the stakeholders.

Deepfakes can be seen as an opportunity, as well as a challenge. Their regulation demands not only a change of the law, but a more general reaction in the society, with technology, policy and ethics. The results of this dissertation indicate that a holistic, balanced and prospective regulatory framework is necessary.

It is essential to regulate deepfakes in India and take collective action. The techno-legal approach with a focus on reinforcing the current frameworks and collaborating on the global level allows India to successfully respond to the challenges of deepfake technology and simultaneously promote innovation and safeguard basic rights.

FOOTNOTES

[1] World Economic Forum, *Global Risks Report* (2020).
[2] European Parliament, “Disinformation and Propaganda – Impact of Deepfakes” (2021).
[3] Electronic Frontier Foundation, “AI and Free Speech Concerns” (2021).
[4] Information Technology Act, 2000.
[5] Indian Penal Code, 1860 / Bharatiya Nyaya Sanhita, 2023.

[6] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

[7] Digital Personal Data Protection Act, 2023.

[8] *Justice K.S. Puttaswamy v. Union of India.*

[9] *Shreya Singhal v. Union of India.*

[10] Internet Freedom Foundation, reports on intermediary liability.

[11] Constitution of India, Art. 19(1)(a).

[12] NASSCOM, AI policy recommendations.

[13] World Bank, digital economy reports.

[14] United Nations, reports on digital governance.

REFERENCES

[1] Stuart Russell and Peter N0rvig, *Artificial Intelligence: A M0dern Appr0ach* (4th edn, Pears0n 2021).

[2] Nigel Smart, *Crypt0graphy Made Simple* (Springer 2016).

[3] Chris Reed, *Making Laws f0r Cyberspace* (0xf0rd University Press 2012).

[4] Ian Walden, *C0mputer Crimes and Digital Investigati0ns* (0xf0rd University Press 2016).

[5] Tal Zarsky, *Privacy and Data Pr0tecti0n in the Digital Age* (Cambridge University Press 2020).

[6] Daniel J. S0l0ve, *Understanding Privacy* (Harvard University Press 2008).

[7] Paul Bernal, *Internet Privacy Rights* (Cambridge University Press 2014).

[8] Vivek S00d, *Cyber Law Simplified* (McGraw Hill 2020).

[9] Justice Yatindra Singh, *Cyber Laws* (Universal Law Publishing 2012).

[10] J0nathan Herring, *Criminal Law: Text, Cases and Materials* (0xf0rd University Press 2022).

[11] W0rld Ec0n0mic F0rum, *Gl0bal Risks Rep0rt* (2020–2024).

[12] NITI Aay0g, *Nati0nal Strategy f0r Artificial Intelligence* (2018).

[13] UNESC0, *Rec0mmendati0n 0n the Ethics 0f Artificial Intelligence* (2021).

[14] Eur0pean C0mmissi0n, *White Paper 0n Artificial Intelligence* (2020).

[15] 0ECD, *Principles 0n Artificial Intelligence* (2019).

[16] Deeptrace Labs, *The State 0f Deepfakes* (2019).

[17] Interp0l, *Gl0bal Crime Trend Rep0rt* (2020).

[18] Br00kings Instituti0n, AI and G0vernance Rep0rts (2021).

[19] Carnegie India, *AI G0vernance in India* (2022).

[20] Internet Freed0m F0undati0n, Rep0rts 0n intermediary liability and digital rights.

[21] Justice K.S. Puttaswamy v. Uni0n 0f India.

[22] Shreya Singhal v. Uni0n 0f India.

[23] Anvar P.V. v. P.K. Basheer.

[24] Karmanya Singh Sareen v. Uni0n 0f India.

[25] G00gle India Pvt. Ltd. v. Visaka Industries.

[26] Ministry 0f Electr0nics and Inf0rmati0n Techn0l0gy – https://www.meity.g0v.in

[27] Press Inf0rmati0n Bureau – https://pib.g0v.in

[28] Supreme C0urt 0f India – https://main.sci.g0v.in

[29] Eur0pean C0mmissi0n – https://ec.eur0pa.eu

[30] Federal Trade C0mmissi0n – https://www.ftc.g0v

[31] NASSC0M – https://nassc0m.in