

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS



Open Access, Refereed Journal Multi-Disciplinary
Peer Reviewed

www.ijlra.com

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner whatsoever for any consequences for any action taken by anyone on the basis of information in the Journal.

Copyright © International Journal for Legal Research & Analysis

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board



Dr. Namita Jain



Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrish Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020). Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.



Avinash Kumar



Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

CRIMINALIZING AI-GENERATED DEEPFAKES IN INDIA: BALANCING FUNDAMENTAL RIGHT OF FREE SPEECH AND PROTECTION FROM HARM.

AUTHORED BY - RISHITA SARKAR¹,
B.COM LL.B., [Hons.],
Indian Institute of Legal Studies, West Bengal

ABSTRACT

There has been an exponential growth of artificial intelligence (AI) in the recent years, which has ultimately resulted in the emergence of hyper-realistic deepfakes raising social or public concerns. While deepfakes can be used innovatively in the entertainment field, it is likely to be misused in a larger scale. Therefore, deepfakes has become a growing challenge to legal rules and moral principles. In India, the rise of AI-generated deepfakes creates a twofold problem i.e. protecting the fundamental right of free speech under Article 19(1)(a) of Constitution of India, 1950 and ensuring safeguard from any form of harm, including defamation, deception, and violation of individuals privacy. This article digs into the current Indian legal framework, scrutinizing the Information Technology Act, 2000 and various other codes which can be invoked in cases relating to deepfake videos, cyberbullying, cyberfraud. Therefore, this study puts forward a harmonious regulatory model that consolidates advanced detection systems to prevent misuse without suppressing creativity and innovation.

Keywords: Artificial intelligence (AI), Article 19(1)(a) of Indian Constitution, Information Technology Act 2000, Cyberbullying, Deepfake videos, Cyberfraud.

INTRODUCTION

Deepfakes are escalating apprehension throughout the whole world including India. Deepfake refers to the video of an individual or group of individuals in which their actual face or body has been digitally converted so that they seem to be someone else, typically used immorally or to spread misinformation about that particular individual or group of individuals. While deepfake holds great capacity for inventive expression, humor, innovation, the exploitation of

¹ B.COM LL.B., [HONS.], INDIAN INSTITUTE OF LEGAL STUDIES, WEST BENGAL

such resources poses a significant threat to an individual's privacy, disrepute, gender-based harassment.

The Indian legal system has been slow-going in directly managing deepfakes. It doesn't have specific laws which explicitly defines or criminalizes deepfakes. Although certain provisions like Section 66E² of Information Technology (IT) Act, 2000 which talks about privacy violation, Section 67 which deals with punishment for publishing or transmitting obscene material in electronic form³. Section 356 of Bharatiya Nyaya Sanhita (BNS), 2023⁴ which addresses the offense of defamation and its punishment. However, they fail in tackling the comprehensive harm caused by AI-generated media.

Implementation of regulatory efforts are made more arduous by the conflict arising between enforcing reasonable restrictions under Article 19(2)⁵ and safeguarding the freedom of speech and expression under Article 19(1)(a)⁶.

Therefore, to address this gap rift, there is a compelling need for appropriate legislation that defines and criminalizes malicious deepfake content and its production and dispersal.

However, a major concern while criminalizing deepfakes is that it could lead to misuse of law to suppress dissention or target opposition political parties. This is because there have been many instances in India where laws that were intended to maintain public order and peace have been used unreasonably, especially against activists, journalists. Therefore, without proper safeguards, anti-deepfake laws could also result as a harmful tool.

On the other side, the potential of deepfake to cause immense harm to the society cannot be ignored. The non-consensual fake content which specifically targets women has already created a great damage to the society as a whole including the younger generation. Therefore, if it is left unregulated, deepfakes could destroy the authenticity of evidence.

The debate over penalizing deepfakes in India is not only limited to technology, it is rather a

² Information Technology Act 2000, Section 66E: Punishment for violation of privacy.

³ Information Technology Act 2000, Section 67.

⁴ Bharatiya Nyaya Sanhita, 2023, Section 356: Defamation.

⁵ Constitution of India, 1950, Article 19(2).

⁶ Constitution of India 1950, Article 19(1)(a).

constitutional and moral debate about the limitation of the powers of state and the individual's rights in the digital era. Regulation is necessary but it must be implemented and drafted carefully to avoid breach of democratic freedoms.

This article includes the complex balance between protecting citizens from Misuse of AI (Artificial Intelligence) and preserving the fundamental right of free speech, contributing an analysis of recent legal framework, enforcement challenges and possible recommendations which would suit the current situation of India's socio-legal context.

IMPACT OF AI-GENERATED DEEPPAKES IN INDIA:

In the recent years, India has witnessed a notable digital change which has ultimately led to multiply the risk of cyberfraud, cybercrime, making and dissenting AI-generated deepfake videos. This gave rise to significant worry in the Indian society. Therefore, the impact of AI-generated deepfake videos can be divided in the following categories:

Impact on individual:

As per the report of several researches conducted relating to the impact of deepfakes, it was found that almost ninety-six percent of the surveyed deepfake videos were about pornographic content which specifically targeted women as victims. It addressed the issue of sexual abuse naming it as "sexual photoshopping"⁷. This type of harassment are not only limited to women; it also includes men, children, and in certain cases even the senior citizens. Therefore, it brings about the sense of anxiety, depression, emotional distress among the victims of such abuse.

Impact on Society:

The AI-generated deepfakes includes the creation of fake content which is hard to detect. This type of contents could be used for damaging the reputation of high influential persons, public figures, deceiving people into sending money for extortion purposes. Therefore, it elevates the risk of causing public chaos. These hyper-realistic deepfakes amplifying their effectiveness and potential impact.

Impact on nation:

Deepfakes also has a remarkable threat to nations as they have the power to exploit elections,

⁷ "Adult Online Hate, Harassment & Abuse"- Report from the U.K.

which ultimately has an adverse effect on the financial market as well as influence diplomatic relations and potentially promote terrorism activities, causing extensive panic among the populations of the affected nations. India has expressed the apprehension regarding deepfake videos. There was an incident where a video of the Prime Minister of India singing garba became an internet sensation, which raised concerns regarding the spread of hatred impacting the dignity and integrity of the nation.

Impact on Judiciary:

There is a potential risk to manipulate the evidence in the course of pendency of the legal proceedings leading to injustice. Deepfakes can be implied through various ways in the legal context. A party involving a lawsuit may create a forged video to influence or manipulate the outcome of the case intentionally. Therefore, the creation of deepfake videos, images stand as a significant challenge for the judicial system as well. A well-known example of such cases is where the photo and the voice of the legendary actor “Amitabh Bachchan” was misused for fraudulent activities, this scam was known as the “KBC” scam.

PROMINENT EXAMPLES OF AI-GENERATED DEEPFAKES IN INDIA:

- In the November of the preceding year, a person named “Muralikrishnan Chinnadurai” was watching an event in Tamil-language which was streaming live in the UK where he noticed something strange. In the livestream, a women named “Duwaraka” was giving a speech who was supposedly dead more than a decade earlier in an airstrike in 2009. Therefore, Mr. Chinnadurai scrutinized the video closely and hence noticed glitches in the video. Therefore, it was clear that there has been use of AI to impersonate someone in place of some other person⁸.
- A content creator named “Shahid Sheikh” was using AI tools to portray various influential persons like cricketers, politicians in characters which has not been seen in the early years.
- In the recent time, there were two videos which went viral in the online platforms showing Ranveer Singh and Aamir Khan supporting Congress party. Hence, they filed complaint stating that they were deepfake videos which was made without their consent.

⁸ BBC Report

- In the current scenario, Instagram reels is also a platform where deepfake videos are used in a large scale. The users tend to enjoy such videos and also share and like it in millions of numbers. It is also one of the significant examples of the harmful impact of deepfakes in India.

EXISTING LEGAL FRAMEWORK IN INDIA

The challenges relating to deepfakes as discussed in the preceding sections highlight the need to modulate the use of deepfakes through legal mechanisms. In terms of Indian legal framework, till now, there has been no such legislations which would specifically deal with the issues of deepfakes. In the absence of specific laws for defining and penalizing deepfakes in India, there are certain laws that can be repurposed to apply for the same issue. These have been discussed henceforward.

Right to privacy:

According to the article 12 of UDHR (1948)⁹ which protects the ‘right to privacy’ as an inherent human right, it is impermissible and unlawful to arbitrarily breach an individual’s honor or reputation. Therefore, it has been solemnly included as a fundamental right to life by virtue of Article 21 of Constitution of India. An individual’s right to privacy includes their capability to exercise control over the dissemination of personal information, which is both necessary and imperative. This also encompasses the unconsented use of deepfakes in any conceivable manner, as it has the potential to wear away one’s standing and unduly encroach upon their personal autonomy¹⁰.

However, there has been a conflict between the social media companies and government of India relating to the implementation of the new Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. Therefore, this conflict must be balanced to bring transparency among them.

Information Technology Laws:

Section 66E of the IT Act of 2000 addresses the violation of privacy through the capture, publication, or transmission of images of an individual’s private area without consent. It aims

⁹ Universal Declaration of Human Rights (UDHR) 1948, Article 12: No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation.

¹⁰ KS Puttaswamy v. Union of India (2017).

to punish such offenders who intentionally violates an individual's privacy in this manner. It implies an imprisonment for a duration of three years or fine up to Rs.2 lakh. Another relevant provision regarding such matter is Section 67 of the IT Act, 2000 which basically deals with the punishment for publishing of spreading obscene material in electronic form. It outlines penalties for such act.

Free speech:

The Indian constitution places a strong stress on the freedom of speech and expression under Article 19(1)(a). This right is not absolute and is subject to reasonable restrictions which lies in the interest of sovereignty, integrity, public order, morality and more. On one hand, the ill-natured deepfakes can be justifiably be included under these restrictions. On the other hand, penalizing all forms of deepfake content also could set threatening precedent for censorship and political dissent, risk of overreach.

Copyright laws:

The Indian Copyrights Act, 1957 and Copyright rules, 1958 provides the framework for protecting copyrights. If a person utilizes copyright material without the permission to create deepfakes, copyright holders have the right to initiate legal proceedings against the offender. Section 51 of the Indian Copyrights Act of 1957 establishes punishments for such offenses and any other act infringing copyright standards.

COMPARATIVE INTERNATIONAL APPROACHES

The regulation of deepfakes is a global issue, where different countries have tried to adopt diverse strategies based on their current situation. However, no single approach provides for a complete remedy. Some countries have recently attempted to curb issues regarding deepfake by establishing certain acts or by taking certain initiatives by collaborating technology and industries. Therefore, it is would be too soon to analyze the impacts or results of such acts or initiatives because it has been implemented in the recent years i.e. 2019 to 2024. However, India can establish a effective approach towards such issue by taking ideas from other countries approach like the US, EU, China.

Unites States:

The Malicious Deep Fake Prohibition Act was introduced in the U.S. in 2019 which intended to criminalize the making and dissemination of deepfake content intentionally specifically

during elections. Deepfakes Accountability Act was introduced in the U.S. House of Representatives in 2023. This bill typically attempted to protect security and integrity of the nation against the possible threats which was posed by deepfake technology, it also aimed to provide legal remedy to the victims of deepfakes. Several other states such as California, Texas and Virginia, have also attempted to enact certain laws regarding the same.

European Unions:

The EU adopted a more deterring regulatory approach. It focuses on both prevention and accountability. The EU Artificial Intelligence Act adopted by the European Union in 2024 is considered as one of the first attempt to regulate artificial intelligence. It provides an elaborate definition of deepfakes, and it also introduces specific protections and remedies in case of violation of the act. However, the AI Act has also inculcated concepts that leave space for interpretations which would help in giving constant development to the act and comply with the needs for any such adjustments.

The EU Act also contains some provisions which makes the scope of the act to be limited which may turn into vagueness.

China:

China has introduced regulations like “Provisions on the Administration of Deep Synthesis of Internet Information Services”, which aimed to govern the making and spreading of deepfake content. It covers a wide range of AI-generated content which also included texts, audio, video. This regulation has a unique characteristic because it focuses on both technology and the capacity of it to have social impact on it. The important aspect of it includes mandatory labeling, traceability. Therefore, it can be stated that China has implemented one the rigorous approach with pre-publication regulation in certain matters.

Singapore:

A recent incident which took place in Singapore involving Prime Minister Lee Hsein Loong, whose likeness was used to promote investment products sets as an example of the extent to which deepfakes can be misused and how realistic they seem to be¹¹. Therefore, a \$20M initiative has been passed in the Singapore Parliament on January 10th, 2024 which mainly

¹¹ INFOCOMM MEDIA DEVELOPMENT AUTHORITY.

aimed to grow new mechanisms to deal with deepfakes and prevent misuse. It intends to bring together technologies and various companies to increase their capability to create a better and safer internet. The CATOS¹² which was launched in the first half of the year 2025 aimed to collaborate industries and exchange knowledge for better detection of deepfake. The approach of Singapore demonstrates the strict intervention of state against matters relating to the misuse of deepfake, which is the reason it was criticized for potential overreach.

Therefore, from the above discussion it can be concluded that India can take cues from the various nations and provide a hybrid approach which could be most efficient in the Indian context because it would include practical solutions to such rigid issue.

RECOMMENDED CHANGES TO CURB AI-GENERATED DEEPPKES:

The following are the proposed changes that must be implied to curb AI-generated deepfakes in India:

Specific legislation:

The parliament must take the initiative to enact a specific law which would define the term “deepfake” and also provide provisions which would criminalize deepfake and also prescribe penalties depending on the seriousness of the harm caused to the victim.

Labelling and watermarking:

The government of India must take necessary steps to inculcate digital watermarking and labelling which would indicate the authenticity of the content. They must also impose liability and penalties on creators those who do not conform to such standards.

Amend Information Technology Act, 2000:

Proper steps must be taken to amend the IT Act, 2000 to explicitly provide provisions regarding criminalizing deepfake contents and also define the term “Deepfake”.

Promoting AI Literacy:

The government or the relevant authorities must take steps to launch awareness campaigns to educate the public regarding the deepfake technology and also make them aware of identifying and reporting such harmful contents. Therefore, it is very crucial to provide AI literacy to the

¹² Centre for Advanced Technologies in Online Safety (CATOS).

citizens of the nation.

Collaboration between government and industries:

This approach has been used by the government of Singapore to curb deepfake contents. Therefore, it is important for the Government of India to promote the collaboration between government and industries to identify, address, and prevent deepfakes in India.

Surveillance system:

A proper tracking system must be established which would solely deal in detecting deepfakes and monitor their activities and also respond to such offenders by identifying them and penalizing such persons.

CONCLUSION

The hike of AI-generated deepfakes have created an intricate legal concern and challenge for the Government of India. While the threat of deepfakes causing harm to individuals, society is a real concern, Indian governments response to it must be balanced between the fundamental right of free speech and safeguarding the public from causing harm. According to the current scenario, it is clearly visible that the Information Technology Act 2000, Bharatiya Nyaya Sanhita 2023 is not capable of meeting the severity of the current situation.

The criminalization of such malicious deepfake contents is a necessity. However, it must be done in such a way that it does not take away the fundamental right of free speech and expression under Article 19(1)(a) of Constitution of India,1950 which is also subject to certain restrictions under Article 19(2).

Another approach which Indian Government must implement is that it should adapt certain policies implemented by the various countries like Unites States, China, Singapore, European Union. For example, Singapore took initiative to collaborate industries and government to detect and curb deepfake contents in the country. Another example is European Union where they implemented an act which solely and completely deals with AI-generated deepfakes. Therefore, taking inspiration from such approaches may result in a better form of hybrid approach which would be more effective.

Therefore, the chief challenge which lies is to strike an equilibrium between the fundamental

rights of the citizens of India and protection of individuals from such harm.

By and larger, the Indian government's attempt to regulate deepfakes must not come at the cost of risking the freedom of speech and expression guaranteed by the Indian Constitution. Maintaining a balance is genuinely an issue. Therefore, it is important to implement specific laws with utter care and responsibility upholding the dignity of the democratic and free society.

BIBLIOGRAPHY

Statutes:

The Constitution of India.

The Information Technology Act, 2000.

The Bharatiya Nyaya Sanhita, 2023.

The Copyrights Act, 1957.

Books and journals:

“Digital Doppelgangers: The rise of Deepfakes & Artificial Intelligence”.

“Navigating the world of Deepfake Technology”.

“Tackling the World of Deepfake Technology”.

IEEE Transactions on Information Forensics and Security.

Journal of Artificial Intelligence Research (JAIR).

ACM Transactions on Intelligent Systems and Technology (TIST).

Online Resources

- Striking the Balance: Navigating Deepfakes and Free Speech <https://share.google/pvqKTnmAeio0O6B66>
- Regulating deepfakes and generative AI in India | Explained - The Hindu <https://share.google/6Ls4s07rfrh9dUINI>
- AI and deepfakes blur reality in India elections - BBC News <https://share.google/1AnSYgXhRUFUHmXo6>
- Deepfake Regulation vs. Free Speech: Should India criminalize AI-generated deepfakes under fundamental rights concerns <https://share.google/QN4Hqe5xVOJ9tJSVv>