INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

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 ofthe 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 2 Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Boardnor IJLRA shall be held liable or responsible in any manner whatsever for any consequences for any action taken by anyone on the basis of information in the Journal.

Copyright © International Journal for Legal Research & Analysis

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

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

ISSN: 2582-6433

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 & Utkrisht 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.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS 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.

www.ijlra.com
Volume 2 Issue 7 | Aug 2023
ISSN: 2582-6433

NAVIGATING THE LEGAL LANDSCAPE OF DEEPFAKES IN INDIA: PUNISHMENTS AND PROTECTIONS

AUTHORED BY - SHYAMASIS SARANGI,
Kirit P. Mehta School of Law, NMIMS Navi Mumbai
&
CO-AUTHOR - NIDHI SHARMA,
Kirit P. Mehta School of Law, NMIMS Navi Mumbai

Abstract:

Deepfake technology poses significant challenges to legal systems worldwide, raising concerns about privacy, misinformation, and digital manipulation. This research paper delves into the intricate legal landscape of deepfakes in India, focusing on punishments for offenders and the protections available to individuals and society. By analyzing existing laws, international collaborations, and technological advancements, the paper explores the effectiveness of legal frameworks in combating deepfake threats. The study emphasizes the importance of raising awareness, implementing stringent punishments, and leveraging advanced technologies to safeguard individuals from the malicious use of deepfakes.

Keywords: Deepfake Technology, Legislative Measures, Rashmika Mandanna

Introduction:

The rapid advancement of deepfake technology has revolutionized the digital landscape, enabling the creation of highly realistic fake videos and images. In India, as in many other countries, the proliferation of deepfakes has raised serious legal concerns. This research paper aims to navigate the legal complexities surrounding deepfakes in the Indian context, focusing on the punishments prescribed for perpetrators and the protections available to potential victims. Understanding the existing legal framework, international collaborations, and technological solutions is crucial in addressing the challenges posed by deepfake threats. The paper explores the evolution of deepfake technology, its implications for privacy and misinformation, and assesses the effectiveness of current legal measures. By examining punishments and protections,

ISSN: 2582-6433

this study provides valuable insights into the strategies required to combat the malicious use of deepfakes and protect the integrity of individuals and institutions in the digital age.

Applications of Deep-fake:

Deepfake technology, while having a broad spectrum of applications, is predominantly used for nefarious purposes, posing significant risks to society, especially for individuals active on social media platforms. It is frequently misused to target celebrities and political leaders, leading to harmful consequences such as revenge, blackmail, and identity theft. Malicious intent is evident in the creation of non-consensual adult content, particularly involving well-known actresses, escalating the issue. Additionally, political figures, including world leaders like Barack Obama and Donald Trump, have been exploited through fake videos, potentially endangering global peace. Despite these negative aspects, there are positive applications of Deepfake technology emerging in various sectors. It has become more accessible, enabling its constructive use in art, film, and social media. For instance, the Dalí Museum utilized Deepfake technology to enhance visitor experiences, allowing interaction with Salvador Dalí's life through artificial intelligence. In advertising and business, Deepfake technology is employed for creative campaigns, such as replicating famous artwork or editing videos efficiently in the film industry. Notably, it aids educational initiatives, with examples like footballer David Beckham promoting malaria awareness in multiple languages. Additionally, Deepfake technology finds utility in the retail sector, offering virtual product experiences, and even in healthcare, generating imaginary data to safeguard patient privacy. Furthermore, it can be harnessed for personalized news presentations and fundraising efforts, leveraging synthesized videos featuring influential personalities to raise awareness and support for various causes. Despite its potential, careful consideration and ethical use of this technology are essential to mitigate its negative impact on society.

Understanding the Legal Framework:

In India, the use of deepfakes raises complex legal questions, primarily falling under the purview of laws governing privacy, defamation, and cybercrimes. The Information Technology Act, 2000, specifically Section 66E, addresses the violation of privacy by capturing, publishing, or transmitting the image of a private area of any person without their consent. This provision can be applied to deepfakes that infringe upon an individual's privacy.

ISSN: 2582-6433

The current legal landscape in India does not specifically address the issue of deepfake videos. While existing laws such as the Information Technology Act 2000 and Section 500 of the Indian Penal Code criminalize the publication of obscene material and defamation, they only cover deepfakes related to sexually explicit content. This limited scope fails to regulate the broader domains where deepfakes can be misused.

In the context of the Right to Privacy, recognized as a fundamental right by the Supreme Court, deepfake videos infringe upon individuals' privacy rights. The court emphasized that privacy safeguards an individual's autonomy and control over various aspects of their life. Deepfakes violate this right by manipulating personal information without consent, impacting both physical and mental privacy. Even without explicit legislation, legal claims against deepfake videos would likely succeed in court due to these violations of privacy rights.

Additionally, the Personal Data Protection Bill 2019, which aims to safeguard personal data, contains provisions that indirectly address deepfakes. The bill defines personal data broadly, encompassing any characteristic of a natural person. Data fiduciaries, whether individuals or companies, must process data lawfully and obtain consent before processing individuals' data. The bill also introduces the "right to be forgotten," allowing individuals to request the removal of unauthorized personal data from the public domain, backed by penalties for violations.

Once the Personal Data Protection Bill is enacted, it is implied that the creation and circulation of unauthorized deepfake videos will be prohibited, offering legal recourse against this emerging threat.

Punishments and Penalties:

The punishments for creating and disseminating deepfakes in India can be severe. Under the Information Technology Act, 2000, Section 66E prescribes imprisonment for up to three years or a fine extending to two lakh rupees, or both, for capturing, publishing, or transmitting private images of an individual without their consent. Moreover, Section 67 of the Act deals with the publication or transmission of obscene material in electronic form, including deepfakes, and can lead to imprisonment for up to three years and a fine.

Additionally, deepfakes can also fall under the ambit of defamation laws. Section 499 and 500

ISSN: 2582-6433

of the Indian Penal Code provide punishments for defamation, which includes imprisonment for up to two years, a fine, or both. If a deepfake is used to tarnish someone's reputation, these provisions can be invoked.

Challenges in Enforcement:

While the legal framework exists, enforcing these laws poses challenges. Identifying the creators of deepfakes can be difficult due to the complex nature of digital technologies. Moreover, the rapid evolution of deepfake techniques makes it challenging for law enforcement agencies to keep pace with the technology.

Identification of Creators:

One of the primary challenges lies in identifying the creators of deepfakes. The intricate web of digital technologies allows malicious actors to conceal their identities effectively. Forensic techniques, although advancing, struggle to keep up with the complexity of deepfake creation methods, making it hard for law enforcement to pinpoint the culprits.

Technological Complexity:

Deepfake technology is constantly evolving, incorporating sophisticated algorithms and machine learning techniques. This rapid evolution means law enforcement agencies need to continuously update their knowledge and tools to detect and combat new variations of deepfakes effectively. Keeping up with these advancements demands significant resources and expertise.

Legal Framework Adaptation:

While a legal framework exists, it often struggles to keep pace with the fast-changing landscape of deepfake technology. Laws and regulations might not be specific enough to address all nuances of deepfake creation, distribution, and malicious intent. Consequently, there could be gaps in the legal system that allow deepfake creators to escape accountability.

International Jurisdiction:

Deepfakes can easily cross international borders through the internet, making it challenging to enforce laws effectively. Jurisdictional issues arise when perpetrators operate from one country, the victim resides in another, and the data servers are located elsewhere. Coordinating international efforts to tackle these cross-border challenges is a complex and time-consuming process.

ISSN: 2582-6433

Public Awareness and Education:

Another challenge lies in educating the public about the existence and potential threats of deepfake technology. Lack of awareness among the general populace hampers reporting efforts, making it difficult for law enforcement agencies to track down instances of deepfake manipulation. Public education campaigns are crucial to encourage vigilance and responsible online behavior.

Resource Allocation:

Enforcing laws against deepfake technology requires substantial resources, including skilled personnel, advanced technology, and financial investments. Law enforcement agencies might struggle with limited budgets and priorities, leading to resource constraints in investigating and prosecuting deepfake cases effectively.

Ethical and Privacy Concerns:

Addressing deepfake technology raises ethical dilemmas and privacy concerns. Striking a balance between combating malicious use of deepfakes and respecting individual privacy rights is a challenge. Crafting laws and policies that protect both privacy and security is a delicate task that requires careful consideration.

Protecting Against Deepfakes:

To combat the threat of deepfakes, raising awareness about the existence of such technology and its potential consequences is crucial. Media literacy programs and educational initiatives can empower people to identify and report deepfakes. Additionally, technological advancements, such as deepfake detection tools, can assist in identifying manipulated content and mitigating the risks associated with these malicious creations.[1]

Media Literacy and Awareness:

Raising awareness about deepfake technology and its potential consequences is fundamental in protecting individuals and society. Media literacy programs can educate people about the existence of deepfakes, how they are created, and the risks they pose. By understanding the

[1] Chenxi Wang, 'Deepfakes, Revenge Porn and the impact on women' (Forbes, 1 November 2019) <https://www.forbes.com/sites/chenxiwang/2019/11/01/deepfakes-revenge-porn-and-the-impact- On-women/#36a482801f53> accessed 15 September 2020

ISSN: 2582-6433

technology, individuals are better equipped to identify suspicious content and discern between real and manipulated information.

Educational Initiatives:

Educational initiatives targeting various age groups, from school students to adults, play a crucial role. Integrating modules about digital literacy, critical thinking, and online safety into school curricula can empower the younger generation to navigate the digital landscape responsibly. Workshops, seminars, and online courses for adults can enhance their awareness of deepfake threats and teach them how to protect themselves from falling victim to misinformation.

Technological Advancements:

Developing and deploying advanced deepfake detection tools is essential for mitigating the risks associated with malicious creations. These tools leverage artificial intelligence and machine learning algorithms to analyze multimedia content, identifying inconsistencies and markers of manipulation. Continuous research and development in this field are necessary to stay ahead of evolving deepfake techniques.

User-Friendly Verification Tools:

Creating user-friendly verification tools can empower individuals to confirm the authenticity of media content. These tools could include browser extensions, mobile apps, or online platforms where users can upload images or videos to check for manipulations. User accessibility and ease of use are crucial factors in ensuring widespread adoption of such tools.

Collaboration with Tech Companies:

Collaboration between government agencies, law enforcement, and technology companies is essential. Tech companies can contribute by investing in research and development of deepfake detection algorithms, implementing stricter content policies, and enhancing their platforms' security features. Public-private partnerships can facilitate the sharing of expertise and resources in the fight against deepfakes.

Legal Framework and Policies:

Strengthening the legal framework and policies related to deepfakes is vital. Clear and specific laws addressing deepfake creation, distribution, and malicious intent can act as a deterrent.

ISSN: 2582-6433

Penalties for offenders should be severe enough to discourage malicious actors. International cooperation is also necessary to address cross-border legal challenges related to deepfake activities.

Ethical AI Development:

Promoting ethical development and use of artificial intelligence is crucial. Ethical guidelines should be established to ensure that AI technologies, including those used in deepfake detection, are developed and deployed responsibly, respecting privacy and human rights. Transparency in AI algorithms and decision-making processes is essential for building trust among users.

Recent Cases:

1. Rise in Fake Political Campaigns:

In 2022, during a state election in India, deepfake videos of political candidates surfaced online, manipulating their speeches and stances on important issues. These videos aimed to mislead voters and damage the candidates' reputations. Several individuals involved in creating and spreading these deepfakes were arrested under the Information Technology Act and IPC Sections related to defamation.

2. Fake Celebrity Scandals:

Deepfake videos involving celebrities engaged in explicit or controversial activities have been widely circulated on social media platforms. In 2023, a prominent Bollywood actress fell victim to such a deepfake scandal, leading to legal action against the perpetrators. The accused were charged under the Information Technology Act and IPC Sections pertaining to privacy violations and defamation.

3. Employment Fraud:

Deepfakes have also been used in employment fraud, where job applicants' resumes and interview videos are manipulated to create false qualifications and work experiences. Companies faced financial losses due to hiring unqualified candidates. Law enforcement agencies intervened, and the culprits were prosecuted under the Information Technology Act for fraud and identity theft.

In a recent alarming incident, renowned actress **Rashmika Mandanna** became embroiled in a

ISSN: 2582-6433

controversy surrounding a viral deepfake video. The video, circulating widely on social media, depicts a woman entering an elevator, her face digitally manipulated to resemble Mandanna's. This incident has stirred significant apprehension, prompting widespread demands for legal intervention. Notably, Bollywood icon Amitabh Bachchan, Mandanna's co-star from the movie "Goodbye," has expressed his distress over the rise of deepfake content and has actively advocated for legal measures to combat this disturbing trend.[2]

Proposed Legislative Amendments:

There have been instances where programs have been created to generate nonexistent human faces. This technology could be misused to produce deepfake videos, which can then be uploaded on social media through fake accounts. Currently, Indian laws do not cover this specific offense, as personation laws require the substitution of a real person, which is not the case with deepfake technology.

To address this issue, potential legislative amendments could be made. One approach could involve modifying the Information Technology (Intermediary Guidelines) Rules 2011. Intermediaries could be instructed to include clauses in their privacy policies, prohibiting users from uploading any form of deepfake content. However, for this prohibition to be effective, the government needs to establish reliable deepfake detection mechanisms.

Additionally, there are no provisions in the current legislation to protect the data of deceased individuals. This gap is concerning, especially considering the possibility of deepfake videos being created to manipulate public opinion or disrupt criminal trials. To rectify this, the law should extend data protection to deceased individuals. The proposed amendments should mandate obtaining consent from the heirs of the deceased before using any of their data for public circulation. Similar provisions, such as those found in the Privacy Act of Hungary and the Spanish Data Protection Act, could serve as models to empower heirs and interested parties to file suits in cases involving the unauthorized use of data belonging to deceased individuals.

[2] https://www.businesstoday.in/technology/news/story/rashmika-mandanna-deepfake-controversy-what-is-a-deepfake-video-and-how-can-you-spot-one-404734-2023-11-06?utm_source=btweb_story_share

ISSN: 2582-6433

Conclusion:

As India grapples with the challenges posed by deepfakes, the existing legal framework offers punishments and protections against their malicious use. However, effective enforcement, coupled with awareness programs and technological solutions, is essential to combat the growing threat of deepfakes and safeguard individuals' privacy, reputation, and security in the digital age.

References:

1. Binayak Dasgupta, 'BJP's deepfake videos trigger new worry over AI use in political campaigns Hindustan Times (New Delhi, 20 February 2020) <https://www.hindustantimes.com/india-News/bjp-s-deepfake-videos-trigger-new-worry-over-ai-use-in-political-campaigns/story-6WPlFtMAOaepkwdybm8b1O.html> accessed 15 September 2020
2. Martin Giles, 'The GANfather: The man who's given machines the gift of imagination' (MIT Technology Review, 21 February 2018) <https://www.technologyreview.com/2018/02/21/145289/the-ganfather-the-man-whos-given Machines-the-gift-of-imagination> accessed 15 September 2020
3. This Deepfake of Mark Zuckerberg Tests Facebook's Fake Video Policies' (Vice, 11 June 2019) <https://www.vice.com/en_us/article/ywyxex/deepfake-of-mark-zuckerberg-facebook-fake-video-Policy> accessed 15 September 2020
4. Kaylee Fagan, 'A Video that appeared to show Obama calling Trump a "dipsh-t" is a warning About a disturbing new trend called 'deepfakes'' (Business Insider, 18 April 2018) <https://www.businessinsider.in/tech/a-video-that-appeared-to-show-obama-calling-trumpa