



INTERNATIONAL LAW
JOURNAL

**WHITE BLACK
LEGAL LAW
JOURNAL
ISSN: 2581-
8503**

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of White Black Legal – The Law Journal. The Editorial Team of White Black Legal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of White Black Legal. Though all efforts are made to ensure the accuracy and correctness of the information published, White Black Legal shall not be responsible for any errors caused due to oversight or otherwise.



WHITE BLACK
LEGAL

EDITORIAL **TEAM**

Raju Narayana Swamy (IAS) Indian Administrative Service **officer**



Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru

and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.



Senior Editor

Dr. Neha Mishra



Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.



Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.



Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM

Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.

More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

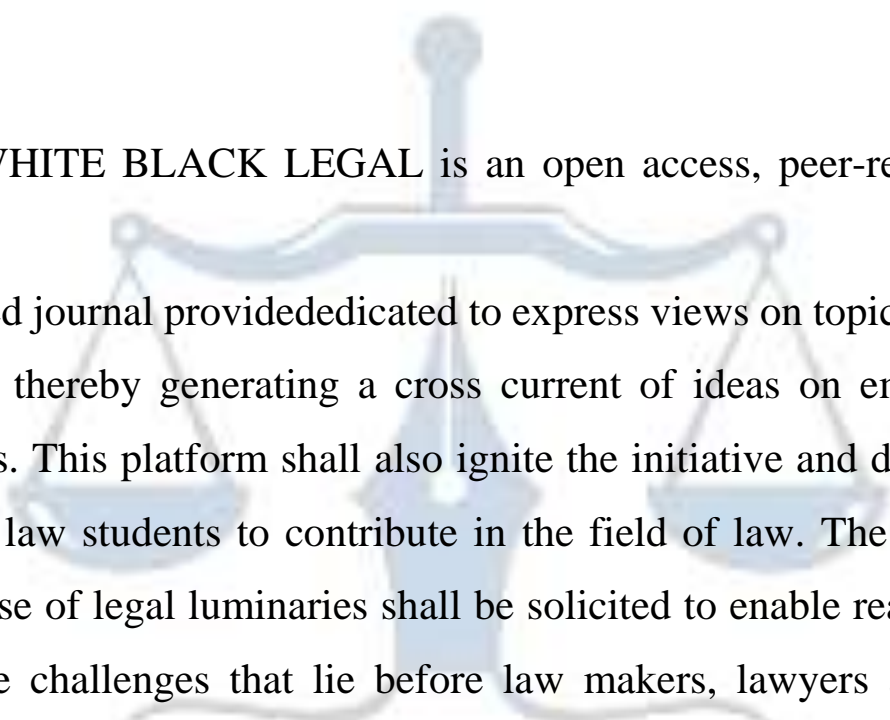


Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US



WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

AI- DEEPFAKES – A MENACE TO PRIVACY IN INDIA: A LEGAL APPROACH

AUTHORED BY - NALLAM ADITYA SRI RAM

Abstract:

Artificial Intelligence which brought technological revolution in the emerging cyber space regime, is being creating both opportunities and challenges in the modern era. One of the contemporary and serious crime being committed with the aid of Artificial Intelligence is Deep Fake. The advent of deepfake technology, which leverages artificial AI to create hyper-realistic but falsified images, videos, and audio, has introduced unprecedented challenges in the digital landscape. In India, the proliferation of deepfakes poses significant threats to privacy, reputation, and even national security, as these manipulations can be used to disseminate misinformation, commit fraud, or defame individuals especially bringing substantial threats to women, emphasising the necessity for effective and ethical standards in this technology. Despite the sophistication of this technology, India's current legal framework under the Information Technology Act, 2000 (IT Act), and related laws, struggles to keep pace with the rapid advancements in AI-driven content creation. This paper explores the implications of deepfake technology in India, and includes the comparative analysis how deep fake is being regulated in EUROPEAN UNION and USA thus explores the necessary changes to be implemented in Indian laws in combatting the deep fake effectively. It also examines the existing cyber laws in India, identifying gaps and proposing necessary amendments to address the specific challenges posed by deepfakes. The discussion includes an analysis of legal precedents, the role of law enforcement, and the need for a comprehensive legal framework that not only deters the misuse of deepfakes but also provides clear avenues for victims seeking redress.

Keywords: Deepfake, Information Technology Act 2000, Artificial Intelligence, USA, European Union.

CHAPTER- II:

2.0. Literature Review:

1. Sarkar, Diya & Sarkar, Sudipta. (2024). *“Combating Deep-fakes in India – An Analysis of the Evolving Legal Paradigm and Its Challenges.”*-

This paper explains deep-fakes, analyses their socio-legal implications, and examines the legal landscape in the US, Europe, and India. The authors aim to provide recommendations to solve the challenges of deep-fake technology and rebuild trust in the digital environment through a comparative review. The authors intend to highlight vulnerabilities in deep-fake technology and emphasise the importance of enacting legislative controls to address these issues.

2. Shraddha pandit and jia singh. *“The East & West of Deepfakes: A Comparative Study of Laws in India & UK.”*

This article emphasises how existing Indian laws are being used in regulating the offence of deepfake. The liability of intermediaries was also discussed in the article. The article draws into a comparative analysis between Indian scenario and UK scenario in combatting the deepfake threat.

3. Anuragini Shrish & Sobhana Komal, *“A Socio- Legal Inquiry on Deepfakes.”*

This paper analyses deepfake technology and its various types. This study examines the impact of deviant actors' usage of deepfakes on multiple institutional levels, drawing on literature on technological affordance and social transformation. The paper proposes public policy solutions to protect vulnerable players from the harmful effects of deepfake technology.

4. Vaishnavi Kulakarni & Bhanusshree Sivaramachandran , *“Tackiling the Multifaceted Legal Dilemmas od Deep Fake Technolgy.”*

This article emphasises the highly interwoven ideas of cyber law and deepfake, putting light on the issues of deepfake pornography, sextortion, fraud, and social engineering attacks. It delves deeper into the Centre's intentions to deal with this in the approaching Digital India era and offers ideas and proposals to improve the regulatory framework by taking cues from laws that are in place around the globe.

5. Amanda Lawson, *“A look at global deepfake regulations.”*

This article provides a global perspective on how deepfakes were being regulated.

2.1. Statement of Research Problem: Significant advancements in Artificial Intelligence have led to the emergence of deepfakes, hyper realistic digital manipulations that pose a significant threat to identity security. India faces significant legal challenges due to the proliferation of deepfake technology, necessitating regulatory action to address the misuse and misuse of such content. However, India's current legal framework does not include specific legislation to handle the creation, distribution, and misuse of deepfake content. The purpose of this study is to comprehend the unique difficulties that deepfakes present in the Indian context and to evaluate possible legislative and policy remedies in order to responsibly handle these problems.

2.2. Objectives of the study: This paper aims to analyse India's current legal responses to deepfakes, compare international approaches and propose regulatory solutions tailored to the Indian context.

2.3. Research Questions:

1. In what ways do deepfakes affect individuals' sense of identity and personal security in each nation?
2. How effective are these regulations in protecting identity security?
3. What strategies are being employed in each country to mitigate the risks associated with deepfakes?

2.4. Scope: This study compares the legal, technological, and policy frameworks in European Union, the US, and India to examine the relationship between AI deepfakes and identity security. The study will include the existing laws in combatting the deepfakes, and the technological responses governed by each country and the effectivity of government measures and the case studies in 3 countries addressing the categories of victims affected by the deepfakes.

2.5. Limitations: The study contains several limitations. The amount of data collected and provided will be meagre as the study is just limited to 3 countries instead of focusing on deepfake at global scale. Obtaining information about deepfake victims may give rise to ethical and privacy issues, particularly in delicate situations. As a result, the scope of some case studies' analysis may be limited. Comparing new technologies across countries is difficult due to their differing legal systems and practices, which necessitate contextual interpretation.

2.6. Research Methodology: The research methodology is based on the doctrinal research. The most precise secondary data had been collected from authentic sources. The data used here has been collected from different articles, journals and legislations.

Introduction: The recent circulation of a deepfake video involving actress Rashmika Mandanna has created a stir in the social media and visualised the threat of using Artificial Intelligence in circulating such deepfake videos. Although the concept of deepfake is not a novel one it gained momentum and attention with the actress video. In addition to the actress issue in January 2024, Sachin Tendulkar, a prominent Indian cricketer, fell victim to deepfake technology. He was spotted advertising an online game with an example of his daughter, Sara Tendulkar, earning Rs. 1.8 million per day by making predictions. The rising prevalence of deepfake technology poses greater dangers to society as a whole by propagating fraudulent videos, which include political threats, financial concerns, and, most obviously, women, who are the most vulnerable segment of the population. Deepfakes are a powerful tool for informational destruction that today's technologically advanced society must contend with, as data-driven economies commonly exchange information through cognitive biases and algorithmic manipulation. It is projected that the issue of truth decay in networked information exchange would get worse every day as deepfake technology proliferates. The necessity for strict rules to shield people from these kinds of hazards is highlighted by the rise in threats and misuse potential in areas like identity theft, character assassination, harm to one's image, reputation, and dependability, and the quick obsolescence of current technologies. Currently in India the offences committed by or through deepfake have been regulated under the legislations of Information Technology Act 2000 and Bhartiya Nyaya Sanhita 2024 (replaced by Indian Penal Code 1860). However, when compared to the other country legislations which are advanced in technology use has framed a separate legislation to combat the dangers of deepfake, India being the 2nd most populated country still faces a lacuna in dealing with the offence of deepfake.

2.7. Deepfake meaning and types: The meaning of the phrase deepfake is Deepfakes, a mix of deep learning and 'fake', are photos, videos, or sounds that are manipulated or generated with artificial intelligence techniques that may show actual or non-existent persons. They are a sort of synthetic medium. In a layman sense, Deepfakes are videos that employ deep learning, artificial intelligence, and photoshopping techniques to produce images of events in order to convey disinformation. A deep-fake is any form of media (audio, video, or else) that has been

partially or completely recreated or altered. The videos are created by combining technology such as GANs (Generative Adversarial Networks) and ML (Machine Learning). A Dutch research claims that GAN technology has advanced to the point where images, audio, or videos processed via it will appear genuine rather than exact replicas due to improvements in content quality and resolution. The word “Deepfake” coined by a reddit user in 2018 who used the reddit forum for the development and application of deep learning techniques for artificially face swapping female celebrities into pornographic videos.¹ The information produced by deepfake can be transmitted through 3 ways by way of video, audio and text. Videos and images that have been altered or generated to present information or behave differently from the original source are referred to as deepfake content. Speech-based authentication systems are vulnerable to Deepfake Audio, especially for individuals whose voice samples are easily accessible, including politicians and celebrities. Articles that appear to have been written by real persons are referred to as textual deepfakes.

2.8. Danger of Deepfake- Created in cyberspace but generating tremors in physical space:

The act of creating deepfakes originally happens in the cyber space. William Gibson coined the term 'cyberspace' in his 1982 short story 'Burning Chrome' to describe a computer-generated virtual reality. However, the word gained popularity in 1984, following its appearance in Gibson's novel Neuromancer. Cyberspace is a compound word, with the initial term 'cyber' derived from the Greek word Kubernetes, meaning pilot, governor, and ruler. The root 'cyber' is also connected to 'cyborg', a term that refers to a human-machine synthesis formed by connecting the human body to advanced high-tech gear. According to Gibson, cyberspace is the term of a real non-space environment, which is characterised by the possibility for the virtual presence and interaction of people through icons, waypoints, and artificial realities. The prevalent use of cyber space has not only created a new dimension for the interaction between people but also developed a serious challenge which involved in increasing of various new crimes being committed in the realm of cyber space. Deep-fakes, which rely on cognitive biases and computational manipulation, pose a significant threat to today's technology-driven civilisation. When comparative to other cybercrimes the concept of deepfake is associated with the increasing sophistication of machine learning has led to the spread of this technology, which is far more difficult to identify and prevent. The suspected deployment of a pornographic video and audio deepfake in 2023, which includes posing as a

¹ Rana, V., Gandhi, A. and Thakur, R., 2023. Deepfakes And Breach Of Personal Data-A Bigger Picture. Law Firm Article.

police officer to threaten and extort money from an elderly individual, was the subject of an intensive investigation by Indian authorities. This frail elderly guy considered ending his life in order to escape social disgrace.²

Although the crime of deepfake has its roots in cyberspace, its effects have since spread to physical space by disrupting a person's identity and causing serious harm to the person's privacy, resulting in a violation of the individual's right to privacy guaranteed by the Indian Constitution under Article-21³. In addition to harming a person's reputation and violating their privacy, deepfakes pose significant hazards to society as a whole, including political and financial threats from the dissemination of misleading information via social media platforms and intermediaries. Deepfake as a crime poses a greater risk to women than men, hence triggering the concept of gender prejudice.

2.9. Political risks: Conducting elections in a fair way is considered to be a hallmark feature of the democratic country. Deep-fakes are a major problem for tackling elections, raising questions about the credibility of democracy, policy formulation, and society as a whole. Political opponents or individuals may release edited recordings of elected officials or prominent personalities indulging in incendiary speech or inappropriate behaviour. Engaging in such behaviours can harm public trust, negatively impact opinion quality, and influence election outcomes. However, the risk is not limited to the sphere of conducting elections but it might result in spread of false information in the country related to the conflict between various community people which will result in violence and effects the peace and safety of the civilians. Deepfakes were being used by the nations in the war to manipulate the people of other country by creating a false video. The recent incident of Volodymyr Zelenskyy, the president of Ukraine, was seen pleading with Ukrainians to give up their weapons in a video message that went viral on social media in March 2022. As a result, the President's office declared the video to be a deepfake as soon as it was acknowledged to be authentic. The video was a watershed moment in information warfare as it was the first time deepfake had been used in a public setting during a war. Even politicians in India were the victims of this highly technical sophisticated crime. Back in 2020, a number of recordings featuring Bhartiya Janata Party

² Man gets caught in deepfake trap, almost ends life; among first such cases in India, ECONOMIC TIMES, <https://economictimes.indiatimes.com/news/newupdates/man-gets-caught-in-deepfake-trap-almost-ends-life-among-first-such-casesin-india/articleshow/105611955.cms?from=mdr> (last updated Nov. 30, 2023, 11:05 AM).

³ Indian Constitution 1950, § 21.

(BJP) leader Manoj Tiwari were shared across several WhatsApp groups, marking the first instance of AI-generated deepfakes being used in political campaigning. Prior to the Delhi elections, Tiwari was heard making derogatory remarks about Arvind Kejriwal in both English and Haryanvi.⁴

3.0. Financial risks: The most vulnerable and hi-tech cybercrime is phishing. Phishing is a sort of cybercrime that involves fooling people into revealing personal information, such as passwords, bank account data, or credit card numbers. Currently phishing has taken a new path with the aid of deepfake technology. Deepfakes are not restricted to the generation of visuals and videos; as previously stated, AI techniques can be used to replicate people's voices in order to carry out financial scams. Approximately 47% of Indian adults have experienced or know of someone who has undergone an AI voice fraud. According to McAfee's research on AI Voice Scams, over 83% of Indian victims reported financial losses, with 48% losing more than INR 50,000. There is a live incident happened in the year 2023 in Kerala where an elderly man fell victim to a video call generated with deepfake technology. The scammer impersonated the victim's old coworker by matching their voice and face. Using the video, the victim transferred money to an account in another Indian state. Authorities have conducted thorough investigations into the incident. This is the first known incidence of a deep phone monetary scam in India. Another significant threat comes from the financial sector, as unsuspecting citizens are intimidated or persuaded to transfer money into a criminal's account using convincing fakes. In such an instance, in April 2024, a businessman from Mumbai, India, was swindled out of Rupees 80,000 in an AI voice cloning scam. The victim was notified that his son had been detained and given a jail sentence over the phone, purportedly from the Indian consulate in Dubai. He was requested to send funds to cover the cost of the bail. The businessman gave the money to the fraudsters because he thought it was his son's voice that was being imitated.

3.1. Invasion of Privacy and Lacuna on personal rights: Individuals in India have the right to privacy under Article 21, which also includes the right to life and liberty. Deepfakes undermine the fundamental right to privacy. A victim's right to privacy may be violated by unauthorised use of personal photos and data, posing a significant challenge in pursuing justice.

⁴ Aartrika bhaumik. (2023). Regulating deepfakes and generative AI in India. <https://www.thehindu.com/news/national/regulating-deepfakes-generative-ai-in-india-explained/article67591640.ece>

Every person is guaranteed the right to privacy as a minimum level of living. The basics of the right to privacy were being shook at the ground level in the cyber world as a result of cyber stalking individuals and data breaches. Deepfake is more commonly connected with the morphing of a person's image, personal information, and videos, which creates privacy problems. With respect to personal rights, they safeguard personalities' names, images, voices, personal qualities, and mannerisms from misuse and commercial exploitation. These rights are vital. Celebrities and famous personalities play an important role in safeguarding their personality traits from being duplicated and presented in public without their permission. In India and other legal jurisdictions around the world, the right to personality is still a relatively new notion. There is no express mention of an individual's right to personality in Indian law, hence this right has grown through legal precedent. In September 2023, the Delhi High Court recognised an individual's right to personality in *Anil Kapoor v. Simply Life India & Ors.*,⁵ and attempted to safeguard Anil Kapoor's personality qualities from being misused by AI technologies to make GIFs, emojis, ringtones, and other modified content. This decision was unique in that it established a precedent for the protection of personal rights in the modern digital era. In this case, 16 entities and the general public were prohibited from using Mr. Kapoor's personality attributes. Previously, in *Amitabh Bachchan v. Rajat Negi & Ors.*,⁶ Mr. Bachchan obtained an interim injunction against the unauthorised use of his voice, name, and picture for commercial reasons. Both of the above decisions effectively granted public personalities the right to personality, giving them control over how their personality features are used.

3.2. Benefits of Deepfakes: Apart from possessing a threat to identity security and damaging a person's fame and spreading falsified and misleading information, deepfakes also possess a potential benefit if users use them in a proper way. Appropriate use of deepfakes provide unique ways for marketing, innovation, training, and operational effectiveness. We go over a few of these below:

3.2.1. Influencer marketing and virtual celebrity endorsements: Companies can use deepfakes to produce realistic influencer copies or showcase virtual celebrity endorsements. This can produce less expensive alternatives to typical celebrity partnerships (such getting an identity licence or consent from the concerned party to deploy deepfakes for a particular

⁵ 2023 LiveLaw (Del) 857.

⁶ 2022 SCC OnLine Del 4110.

purpose), all the while having a significant influence on consumer perception. Deepfakes could potentially be used by influencers and celebrities to improve their public personas and more effectively market their personality rights.

3.2.2. Multilingual communication: Deepfakes can be used to provide multilingual communication tools for companies that operate internationally or in several geographic locations. By removing linguistic obstacles, this promotes efficient communication with a variety of clientele

3.2.3. Digital avatars for video games and movies: Deepfakes may be used to produce incredibly lifelike digital avatars for the video game and movie industries. In turn, deepfakes can help the entertainment industry expand by improving visual effects and producing believable characters. Moreover, deepfakes could be useful in safeguarding gamers' privacy when they play online.

3.2.4. Virtual concerts and performances: Deepfake technology enables musicians and artists to produce virtual concerts and performances. As a result, current opportunities can be greatly increased, and regular interaction with audiences throughout the world is possible⁷.

3.3. Liability of Intermediary in Deepfake works: The question of intermediary liability for content submitted on online platforms/websites is a widely disputed topic around the world. There are differing perspectives on how and under what conditions platforms can be held accountable for the mode and manner in which they are utilised by consumers. The problem of intermediary liability arises in the context of deepfakes and AI-generated content on the internet. The question is whether the Generative-AI platform can be held accountable for the usage of its platform to create deepfake and/or satirical content. With respect to the intermediary liability the Indian ministry of Electronics and Information & Technology (MeitY) issued an advisory notice to all intermediaries after the viral circulation of the actress Rashmika Mandanna's Deepfake video. On 1-3-2024, the Ministry of Electronics and Information Technology ('MeitY') issued an advisory for all intermediaries/platforms under the Information Technology Act, 2000 and Information Technology (Intermediary Guidelines and

⁷Can Deepfakes be leveraged responsibly ?. (2024). Dr. Deborshi Barat , Reshma (Vaidya) Gupte and Nupur Agrawal. <https://www.snrlaw.in/can-deepfakes-be-leveraged-responsibly/>

Digital Media Ethics Code) Rules, 2021, as a continuation of the advisory dated 26-12-2023. Rule 3 of the aforesaid advisory notice speaks about the intermediary action in accordance with deepfake. The rule states that if any intermediary uses software/other computer resources to permit and facilitate the creation/generation/modification of synthetic data that can be used as misinformation or deepfake, such synthetic data should be labelled/embedded with a permanent unique metadata or identifier, in such a way that such label, metadata, or identifier can be used to identify the source and creator/first originator of such misinformation/deepfake. Further the intermediary or social media platforms should compliance with the following steps:

- To ensure that the usage of Artificial Intelligence model/LLM/Generative AI, software, or algorithm on or through its computer resource does not allow users to host, display, upload, change, publish, transmit, save, update, or share any illegal content.
- To ensure that their computer resources do not allow for bias or discrimination or endanger the integrity of the election process, including the use of Artificial Intelligence models/LLM/Generative AI, software, or algorithms.
- The use of under-testing / unreliable Artificial Intelligence model /LLM/Generative AI, software, or algorithm, as well as its availability to users on the Indian Internet, must be done with the explicit permission of the Government of India and only after appropriately labelling the possible and inherent fallibility or unreliability of the output generated.

In addition to the legislation compatibility, the Ministry of Electronics & Information Technology (MeitY) had laid down a few guidelines which prioritizes the role of intermediaries while dealing with the deepfakes:

- Ensure that due diligence is taken and reasonable measures are made to uncover disinformation and deepfakes, and in particular, information that breaches the terms of rules and regulations and/or user agreements and
- Such cases are promptly addressed, well within the deadlines specified by the IT Rules 2021.
- Users are prevented from hosting such information/content/Deep Fakes.
- Remove any such content within 36 hours of being reported. Ensure prompt action, well within the deadlines specified by the IT Rules 2021, and disable access to the content/information⁸.

⁸ MeitY issues advisory on Misinformation and Deepfake mandating unique metadata. (2024). Kriti.

3.6. Tackling of Deepfake in India: In Indian scenario there was no a separate legislation which neither regulates AI nor deepfake. In the Mandanna case, the Delhi Police Special Cell reportedly filed a FIR against unknown persons under Sections 465 (forgery) and 469 (forgery to harm a party's reputation)⁹. Furthermore, in the prevailing case involving Mr Sachin Tendulkar, Section 500 [Punishment for Defamation] of the IPC was used against the gaming site owner who was responsible for spreading the deepfake video. It should be highlighted that, while the malicious use of deepfakes may constitute criminal defamation under Section 500¹⁰ of the IPC, the legal position gets complicated when the deepfake depicts genuine individuals.

The existing Information Technology (IT) Act 2000 and newly enacted Bhartiya Nyaya Sanhita 2023 are the two legislations which were being used to tackle the deepfake challenge. Deepfake coming in the notion of cyber crime is predominantly dealt under the provisions of the Information Technology act 2000. The laws and the provisions governing the deepfake are:

| Sl.No. | Name of the legislation | Provision details |
|--------|----------------------------------|--|
| 1 | Information Technology Act, 2000 | 66D. Punishment for cheating by personation by using computer resource– Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees. ¹¹ 66E. Punishment for violation of privacy– Whoever, intentionally or knowingly captures, publishes or transmits |

<https://www.scconline.com/blog/post/2024/03/07/meity-issues-advisory-on-misinformation-and-deepfake-legal-news/>

⁹ PTI (2023). DCW Seeks Action Taken Report from Delhi Police On Rashmika Mandana Deep Fake Video. The Hindu. [online] 10 Nov. Available at: <https://www.thehindu.com/news/cities/Delhi/dcw-seeks-action-taken-report-from-delhipolice-on-rashmika-mandana-deep-fake-video/article67521073.ece> (Last Accessed 14 January, 2024)

¹⁰ Indian Penal Code 1860, S 500

¹¹ Information Technology Act 2000, § 66D

| | | |
|--|--|---|
| | | <p>the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.¹²</p> <p>67. Punishment for publishing or transmitting obscene material in electronic form.—Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.¹³</p> <p>67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.—Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven</p> |
|--|--|---|

¹² Information Technology Act 2000, § 66E

¹³ Information Technology Act 2000, § 67

| | | |
|----|---|--|
| | | years and also with fine which may extend to ten lakh rupees. ¹⁴ Section 67 B – punishment for publishing or transmitting of material depicting children sexually explicit act/pornography in electronic form. ¹⁵ |
| 2. | Indian Penal Code 1860 ¹⁶ | Sec- 499: Criminal Defamation Section- 509: Word, gesture or act intended to insult the modesty of a woman. Sections 465 (punishment for forgery) and 469 (forgery for purpose of harming reputation) |
| 3. | Bhartiya Nyaya Sanhita 2023 | Section- 356(1) & (2): Defamation Section 79: Word, gesture or act intended to insult the modesty of a woman. |
| 4. | Indian Copyright Act 1957 | Section- 51- Deemed infringement. ¹⁷ |
| 5. | Protection of Children from Sexual Offences Act, 2012 (POCSO) 2012 | Sections 13,14 & 15 to protect the rights of women and children. |
| 6. | Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 | Imposes obligations to expeditiously remove misinformation, failing which liability is imposed. |
| 7. | Digital Personal Data Protection Act 2023 | Data Protection and Privacy |

The Digital Personal Data Protection Act of 2023 (the "DPDP Act") defines personal data as "data about an individual who is identifiable by or in relation to such data." This refers to both directly and indirectly identifiable information. Thus, if an image contains information that can be used to identify a specific individual, for example, when paired with other data or identifying traits such as facial features, such photographs and videos would be considered personal information.

¹⁴ Information Technology Act 2000, § 67A

¹⁵ Information Technology Act 2000, § 67B

¹⁶ Indian Penal Code, 1860. Act No. 45 of 1860.

¹⁷ Indian Copyright Act 1957, § 51.

Furthermore, the DPDP Act has extraterritorial applicability, which means it applies even if the author of deepfake films is based outside of India.

Additionally, this law seeks to grant people the ability to designate another person to exercise their rights in the event of their incapacity or death. Therefore, such provisions require prior consent from the heirs of such deceased individuals and grant them the right to sue in the event of violations when deepfake videos of them—such as politicians or spiritual leaders—are circulated with the intention of influencing the beliefs of the masses.

According to a recent report, Journalist Mr. Rajath Sharma after his personal encounter with a malicious deepfake film, he filed a public interest litigation (PIL) in the Delhi High Court, calling on the Ministry of Electronics and Information Technology (MeitY) to identify and restrict sites that enable the creation of deepfakes. The court's recognition of the issue's importance suggests that political parties have voiced similar worries. Sharma's PIL further urges platforms to disclose AI-generated content in a clear and understandable manner and seeks for the appointment of a government nodal authority to handle deepfake concerns. He points out important flaws in the law as it stands, especially the Digital Personal Data Protection Act of 2023, which he claims falls short in addressing the problems caused by deepfakes. The Delhi High Court on August 28, 2024, the Delhi High Court in response to the aforesaid PIL noted that deepfakes will pose a significant threat to society and that the Centre has to "get working on this."¹⁸

Acting Chief Justice Manmohan and Justice Tushar Rao Gedela stated during the hearing of two petitions against the lack of regulation of deepfake technology in the nation that "it [deepfake] is going to be a serious menace in the society."

A LOOK AT GLOBAL SCENARIO:

EUROPEAN UNION: The European Union (EU) has taken a proactive approach to regulating deep-fakes, urging for further study on identifying and preventing them. The latest Artificial Intelligence Act of 2024 (AIA) in the EU has taken a very proactive approach to combating deepfakes. Along with labelling deep-fakes as "manipulated or synthetic audio, image or video

¹⁸ Start working against deepfakes, Delhi HC tells Centre. The Hindu. (online). Aug 29 Available at <https://www.thehindu.com/news/cities/Delhi/start-working-against-deepfakes-delhi-hc-tells-centre/article68576870.ece>

content that would falsely appear to be authentic or truthful, and which features depictions of persons appearing to say or do things they did not say or do, produced using AI techniques, including machine learning and deep learning.

The EU AIA addresses the issue of deep-fake with three key components:

- a) A precise definition of deep-fake (Article 3(60));
- b) Transparency requirements for AI suppliers and deployers, commonly known as deepfake makers (Article 50);
- c) Recitals 132-137.

According to Article 3(60) of the text, "deep-fake" refers to artificially manufactured or altered images, audio, or video content that closely resembles actual people, places, objects, events, or entities. The AIA enforces stricter standards for higher levels of risk. The EU has suggested regulations requiring transparent labelling of artificially created content to combat deep-fakes.

It has been duly recognised under the recently established AIA. The AIA's 133 recital emphasises the importance of adaptation to varied information formats, sophisticated technology, and AI capabilities. This ensures effective adherence for service providers, especially those handling diverse materials and advanced technologies. Recital 133 emphasises the importance of precise, compatible, and efficient methods for tagging and identifying content. Their objective is to verify the legitimacy of content and monitor its source. Individuals who have had their personal data manipulated in a deepfake scenario, also known as "data subjects," may have the right to erasure under Article 17 GDPR if the information is genuine and reliable.

The EU has mandated that social media networks remove disinformation, including deep-fakes. The Code of Practice on Disinformation, amended in June 2022 under the Digital Services Act 2022 (DSA), addresses the subject of deep-fakes. Since February 2024, the DSA 2022 applies to all EU member states, affecting both online content creators and intermediaries. Violations of these regulations may result in fines up to 6% of their global income.

The EU has developed the world's first comprehensive AI law to fight the growing threat of deep-fakes, complementing existing regulations and initiatives. These regulations aim to limit

the use of deep-fake technology in disinformation governance, protect personal information, and regulate artificial intelligence. The European Commission's AI regulatory framework is crucial for enforcing laws against deep-fakes, while its implementation is still pending.

| Sl.No. | | Statute | Year | Deepfake related content |
|--------|--|------------------------------------|------|--|
| 1 | | The Artificial Intelligence Act | 2024 | A comprehensive regulatory framework for AI that encompasses the issue of deep-fake technology |
| 2 | | The Digital Services Act | 2022 | It regulates online intermediaries and platforms. |
| 3 | | The AI Regulatory Framework | 2021 | Labelling deep-fake content to warn users of modified footage. |
| 4 | | General Data Protection Regulation | 2018 | Data Protection and Privacy |

Deepfake laws in USA: The United States of America (U.S.A.) took the lead as the first nation to address the rise of artificial intelligence technology. The Malicious Deep Fake Prohibition Act was passed by the US Congress in 2018. This law is significant because it represents the first attempt to provide a legal definition for the phrase "Deep-fake". The term 'deep fake' means an 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. In February 2024, an audio deepfake surfaced that resembled the voice of US President Joe Biden. The audio sample was utilised in an automated phone call to Democratic voters in the US state of New Hampshire. In the bogus message, an AI-generated facsimile of Biden's voice is heard asking people not to vote in the state's primary election. In 2019, the DEEP-FAKES Accountability Act was formally presented. Deepfake was defined in the modified DEEP FAKES Accountability Act presented by Representative Yvette D. Clark (D-NY) in 2023.¹⁹

¹⁹ Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act of 2023, H.R. 5586, 118th Cong. (1st Sess. 2023).

It is defined as follows:

Any video recording, motion-picture film, sound recording, electronic image, photograph, or any technological representation of speech or conduct substantially derivative thereof—

- A. that seems to authentically depict any speech or conduct of a person who did not in fact engage in such speech or conduct; and
- B. whose production was largely dependent upon technical means rather than another person's ability to physically or verbally impersonate such person—is defined as a deepfake in Section 2, subsection(n)(3) of the Bill.

However, the public voiced complaints and worries about its vague definitions and possible violations of the First Amendment to the US Constitution. The proposed DEEP FAKES Accountability Bill includes a criminal penalty of fines, imprisonment for up to five years, or both. The civil penalty consisted of "up to \$150,000 per record or alteration and appropriate injunctive relief." The proposed bill provided "a civil penalty of up to \$150,000 per record or alteration, as well as appropriate injunctive relief" for modifying disclosures. Despite the failed proposals, in a 2022 Presidential Memorandum, President Biden established special task groups to combat cybercrime. These task forces combat online harassment and abuse, especially gender-based violence, by employing deepfakes, non-consensual distribution of private photographs, cyber stalking, and sextortion. Currently in the federal view of the US, there was no legislation to regulate deepfake content but states like California and Texas have enacted their own legislations for safeguarding the personal identity from deepfake content. In 2019, Texas became the first jurisdiction in the US to criminalise the creation and dissemination of deep-fake videos intended to hurt politicians or influence elections. Creating and distributing a deep-fake film within 30 days of an election is now a Class A misdemeanour in Texas. The goal is to injure a candidate or manipulate the outcome. The maximum punishment for this infraction is one year in county jail and \$4,000 fine.

| Sl.NO. | Legislation | Regulation | Year | Deepfake related content |
|--------|-------------|-------------------------------------|------|--|
| 1 | Federal | Malicious Deep-fake Prohibition Act | 2018 | Set up criminal office relating to deep-fake election media. |
| 2 | Federal | Deep-fakes Accountability Act | 2019 | Decides civil & criminal accountabilities for altered media. |
| 3 | Federal | The Deep-fake Report | 2019 | Mandates reporting annually on |

| | | | | |
|---|--------------|-------------|-------|---|
| | | Act | | deep-fake pornography |
| 4 | State- Texas | Tex. SB 751 | 2019. | Deep-fakes for causing harm to electoral process or public officials. |

Conclusion: In the Indian context, the emergence of deepfake technology poses both a challenge and an opportunity. Deepfakes can be inventive and imaginative, but when used improperly, they pose serious risks to national security, privacy, and public confidence. Deepfake regulation poses difficult problems that call for a careful strategy that strikes a balance between security, privacy, and freedom of speech. Deepfake technology presents special risks in India, where there is a high prevalence of digital media consumption and a high risk of disinformation, especially with relation to political stability, personal privacy, and reputational damage.

In conclusion, India has the chance to establish a legislative framework that encourages responsible AI innovation while also guarding against the malevolent use of deepfakes. India may enact efficient laws that improve digital safety, protect democratic integrity, and guarantee that deepfake technology is utilised morally and productively by embracing a hybrid model influenced by both US and EU strategies.

CHAPTER- IV. Policy Considerations & Future Recommendations:

- ✓ Aside from developing legislation to prohibit the misuse of this technology, another important challenge is determining whether a video is phoney in the first place. To date, with every flaw discovered in deepfakes to aid detection, a better version of the algorithm has been produced, eliminating the prior flaws. As a result, the government and other regulatory authorities must take steps to confirm the authenticity of publicly available films.
- ✓ The Indian government can mandate that internet service providers, social media platforms, and other online intermediaries monitor and report suspicious deepfake activity to law enforcement in real-time. This allows for early detection and intervention, preventing the spread of hazardous deepfakes.
- ✓ Personal Accountability: It is incumbent upon each individual to utilise prudent discernment when absorbing information from the internet. Think things through before

you share anything on social media. It is imperative to take part in the battle against the "infodemic" by utilising the internet appropriately.

- ✓ Establish a Research and creation Wing: Given that DARPA has pioneered the creation of deepfake detecting technologies, India ought to consider establishing a dedicated research and development agency along similar lines.
- ✓ Boost Legal Frameworks: To ensure that identity theft related to deepfake is adequately prosecuted, comprehensive laws should be adopted in South Korea, the US, and India.
- ✓ Boost Technological Capacity: To increase technological readiness, governments should fund AI-based deepfake detection systems and promote public-private collaborations.
- ✓ Increase Public Awareness: Public education campaigns about the dangers of deepfakes, especially with regard to identity security, should be expanded in all three of the aforementioned countries.
- ✓ Encourage International Collaboration: Because deepfake-related crimes are transnational in nature, international cooperation is crucial to their solution. Building a cohesive response can be facilitated by exchanging technology breakthroughs, legal frameworks, and best practices.

CHAPTER- V: REFERENCES:

1. Sarkar, Diya & Sarkar, Sudipta. (2024). Combatting Deep-fakes in India – An Analysis of the Evolving Legal Paradigm and Its Challenges. 15.
2. ANURAGINI SHIRISH AND SHOBANA KOMAL. A SOCIO-LEGAL INQUIRY ON DEEPFAKES. California Western International Law Journal, Vol. 54, No. 2 [], Art. 6.
3. Kailyn Slater and Akriti Rastogi. (2022). Deep-Rooted Images: Situating (Extra) Institutional Appropriations of Deepfakes in the US and India. ISSN 1930-014X Volume 19, Issue 1. doi: 10.32855/fcapital.202201.007.
4. Can Deepfakes be leveraged responsibly ?.(2024). Dr. Deborshi Barat , Reshma (Vaidya) Gupte and Nupur Agrawal. <https://www.snrlaw.in/can-deepfakes-be-leveraged-responsibly/>.
5. MeitY issues advisory on Misinformation and Deepfake mandating unique metadata. (2024). Kriti. <https://www.sconline.com/blog/post/2024/03/07/meity-issues-advisory-on-misinformation-and-deepfake-legal-news/>

6. Vig, Shinu. "Regulating Deepfakes: An Indian perspective." *Journal of Strategic Security* 17, no. 3 (2024) : 70-93. DOI: <https://doi.org/10.5038/1944-0472.17.3.2245> .
7. Dr.Sarigama.R.Nair, THE EMERGING THREAT: DEEPFAKE AND WOMEN IN INDIA. (2024). *IJCRT* Volume 12, Issue 5.
8. SHRADDHA PANDIT AND JIA SINGH. *The East & West of Deepfakes: A Comparative Study of Laws in India & UK*. Volume-6. Issue-3. DOI: <https://doi.org/10.1000/IJLSI.112058>.
9. Sungshin (Luna) Bae. (2024). AI is fuelling a deepfake porn crisis in South Korea. What's behind it – and how can it be fixed? <https://theconversation.com/ai-is-fuelling-a-deepfake-porn-crisis-in-south-korea-whats-behind-it-and-how-can-it-be-fixed-238217>.
10. Aartrika bhaumik . (2023). Regulating deepfakes and generative AI in India. <https://www.thehindu.com/news/national/regulating-deepfakes-generative-ai-in-india-explained/article67591640.ece>.
11. Indian Penal Code, 1860. Act No. 45 of 1860.
12. The Bharatiya Nyaya Sanhitha, 2023. Act No. 45 of 2023.
13. Indian Copyright Act, 1957. Act No. 14 of 1957.
14. DeepTrace, *The State of Deepfakes, Landscape, Threats, and Impact* https://regmedia.co.uk/2019/10/08/deepfake_report.pdf.
15. 2023 LiveLaw (Del) 857.
16. 2022 SCC OnLine Del 4110.

WHITE BLACK
LEGAL.