Page 864 - 869 **DOI:** *https://doij.org/10.10000/IJLMH.119190*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 8 | Issue 2

2025

Blurred Boundaries: When AI Challenges Consent and Privacy

RATTANDEEP SINGH[1], ATHER NAZIR[2] & SARABJOT KAUR[3]

ABSTRACT

The drastic rise of AI-Generated content specifically deep-fake pornography is posing a significant threat to mental health, privacy and societal dignity. This is is further boosted by the conventional legal frameworks. These are classified into various tools such as the DeepFace Lab and they exploit individuals by creating a replica of their facial features and using the same for explicit content. Internationally multiple nations are implementing various enactments and imposing regulations which display the need of having a multi-faceted approach to mitigate deep-fake risks. This short note displays the importance of initiating an appropriate balance between innovation with safeguards to curb the exploitation of AI-Technology.

Keywords*: Deepfake, Ai content, Chatgpt, ai pornography.*

I. INTRODUCTION

The viral nightmare where fiction becomes reality. Imagine waking up one morning to discover that an explicit video of yourself is spreading across the internet like wildfire. But you never filmed it and never consented to it. It's like being trapped in a digital scandal that is not real but for others real enough that may ruin your life. I

In October 2023, a deep-fake video of Rashmika Mandanna (South Indian Actress) surfaced on various online platforms superimposing her face onto explicit content. Within a span of 24-Hours, it spread across Instagram, Telegram, and X which sparked outrage. The Culprit was a 24-year-old engineering graduate from Guntur, Andhra Pradesh, who did this just for the sake of gaining followers for a fan page.[4]

This was not an isolated incident but rather a warning shot as Deep-fake pornography became the darkest corner of AI Innovation where the women are the main targets and victims take

[1] Author is a student at University Institute of Legal Studies, Chandigarh University, India.
[2] Author is a student at University Institute of Legal Studies, Chandigarh University, India.
[3] Author is a student at University Institute of Legal Studies, Chandigarh University, India.
[4] Times of India, Rashmika Mandanna Expresses Her Heartfelt Gratitude to the Delhi Police for Arresting Creator of Her Deepfake Video, https://timesofindia.indiatimes.com/entertainment/hindi/bollywood/news/rashmika-mandanna-expresses-her-heartfelt-gratitude-to-the-delhi-police-for-arresting-creator-of-her-deepfake-video/articleshow/107018620.cms? (last visited Mar. 18, 2025).

 [ISSN 2581-5369]

numbers in provided 96% of all deep-fake content is pornographic and 99% of those are women.[5]

The impact of deep-fake pornography is not just about defaming someone but more than that. It's a direct assault on privacy, dignity, and mental health. Victims face public humiliation, professional setbacks, blackmailing for different demands and emotional trauma that is rare to heal in such circumstances. When these victims seek justice, they are often hit with a legal dead-end.

Why? Reason being India's legal framework was not designed for an AI-Driven World. Currently, the Bhartiya Nyaya Sanhita (BNS), 2023, replaces the Indian Penal Code, but does it address AI-generated abuse? The loopholes are glaring.

II. UNDERSTANDING DEEPFAKE PORNOGRAPHY

Deep-fakes are synthetic media where an Artificial Intelligence (AI) smoothly replaces the person's resemblance of facial features with another in images or videos tools like "DeepFace Lab"[6] or the Chinese App "Zao"[7] are prime examples. This technology leverages deep learning algorithms to make hyper-realistic content which makes it extremely challenging to find a difference between authentic and fabricated media. It uses deep learning algorithms and generative adversarial networks (GANs)[8] and this makes the altered image, audio and video almost impossible to distinguish them as fact from the fabricated content.

Originally, it was developed for cinematic effects and voice synthesis which now is widely being misused specifically for political misinformation, financial fraud and non-consensual pornography. Globally, more than 500,000 content of video and voice altered deep-fakes were shared on social media platforms in 2023. By 2025, this number is expected to reach 8 million, consistent with doubling every six months.[9]

Over, 75% of Indians have encountered deep-fake content in the past year in which only 30% were confident to have the AI content distinguished from the Original one. Approximately 30% of Indians reported that 25% or more of the videos or content they are consuming is later on

[5] The State of Deepfakes: Landscape, Threats, and Impact (2019), https://regmedia.co.uk/2019/10/08/deepfake_report.pdf (last visited Mar. 18, 2025).

[6] iperov, DeepFaceLab, GitHub, https://github.com/iperov/DeepFaceLab (last visited Mar. 18, 2025).

[7] BBC News, 'Deepfake' app causes fraud and privacy fears in China, https://www.bbc.com/news/technology-49570418 (last visited Mar. 18, 2025).

[8] viso.ai, Guide to Generative Adversarial Networks (GANs) in 2024, https://viso.ai/deep-learning/generative-adversarial-networks-gan/ (last visited Mar. 18, 2025).

[9] authentic, It's Deepfake Season: Where to Expect Deepfakes Across Your Digital Day, https://www.authenticid.com/biometrics/its-deepfake-season-where-to-expect-deepfakes-across-your-digital-day/ (last visited Mar. 18, 2025).

 [ISSN 2581-5369]

found to be AI Generated.[10]

Deep-fake scams are increasing as the technology advances and becomes more accessible these frauds are difficult to trace and detect especially in real-time video calls. In Kerala, A person lost ₹40,000 in an AI-Generated deep-fake Whatsapp fraud in which the scammer impersonated a former colleague using AI Technology and requested money in the name of medical emergency.[11]

These statistics and insights underscore the growing threat of deep-fakes in India and Globally and Addressing this issue requires a multifaceted approach involving technology, education, and legislation.

III. GLOBAL LEGAL PERSPECTIVES: HOW OTHER NATIONS ARE RESPONDING

The global hike in deep-fake technology has promoted various nations to implement legal provisions that deal with challenges and barriers created by AI-generated non-consensual content. There is an urgent need to address such issues either by considering global models or legislation from different countries ensuring the protection of individual rights, and maintaining digital integrity and transparency.

Legislative efforts in the United States at the Federal Level are being conducted acts like the DEEPFAKES Accountability Act[12] aim to protect national security and provide legal recourse for victims of harmful deep-fakes along the NO FAKES Act[13] seeks to empower victims by allowing individuals to exercise rights over digital replicas of their voice and likeness. A country with an unwritten constitution the United Kingdom's Online Safety Act,[14] effective from January 31, 2024, criminalizes the sharing of any type of AI-generated content without consent and assures the tech companies to remove illegal content and any explicit AI-generated content and it also ensures in fines or operational restrictions under non-compliance scenario. Measures like mandates requiring deep-fake content to carry clear watermarks as well as compulsory real-

[10] Over 75% of Indians exposed to deepfake videos in the last 12 months, only fraction realised AI trickery Firstpost, https://www.firstpost.com/tech/over-75-of-indians-exposed-to-deepfake-videos-in-the-last-12-months-only-fraction-realised-ai-trickery-13764084.html (last visited Mar 18, 2025)

[11] India Today, Kerala man loses Rs 40,000 to AI-based Deepfake WhatsApp fraud, all about the new scam, https://www.indiatoday.in/technology/news/story/kerala-man-loses-rs-40000-in-ai-based-deepfake-whatsapp-fraud-all-about-the-new-scam-2407555-2023-07-17 (last visited Mar. 18, 2025).

[12] DEEPFAKES Accountability Act, H.R. 5586, 118th Cong. (2023), https://www.congress.gov/bill/118th-congress/house-bill/5586/text (last visited Mar. 18, 2025).

[13] Dean, Salazar Introduce Bill to Protect Americans from AI Deepfakes, https://dean.house.gov/2024/9/dean-salazar-introduce-bill-to-protect-americans-from-ai-deepfakes (last visited Mar. 18, 2025).

[14] CSIS, A New Chapter in Content Moderation: Unpacking the UK Online Safety Bill, https://www.csis.org/analysis/new-chapter-content-moderation-unpacking-uk-online-safety-bill (last visited Mar. 18, 2025).

 [ISSN 2581-5369]

ID verification for the users that create such content have been implemented in China.[15]

India on the contrary faces a critical juncture in addressing the issues created by deep-fakes. Considering global examples, the country could consider the implementation of legislation specifically aligned to Deep-fake issues which target the creation and sharing of non-consensual AI-generated content along with this AI Detection Tools and block-chain tracking can help to identify and trace the origin of deep-fakes. There is an urgent need for amalgamating Technology and Legal frameworks to deal with untraceable content creators.

Regulating access to the tools that are capable of creating deep-fake content by requiring their real ID can be another measure that if infused within India's Digital Personal Data Protection Act, 2023 (DPDP Act)[16] can be extremely useful. This will ensure fast removal of such content and identifying the content creator. The EU's GDPR (General Data Protection Regulation)[17] serves as a strong model which regulates the unauthorized use of personal data in deep fakes. Combining strict data rules and legislation with AI restrictions can help India curb deep-fake abuse while assuring ethical AI use.

IV. DEEPFAKE TECHNOLOGY: A CATALYST FOR SEXISM, OBJECTIFICATION, AND DIGITAL MISOGYNY

A major aggravation for sexism and chauvinism can be deep-fake content pro-longing the stigmatization of women in the world. Deep-fake content has the latent to subject the dupe, in maximum cases women, into becoming the aims of voluptuous objectification, with deep-fakes being exploited to publicize non-consensual explicit content of such women. Hence, the occurrence of misogynistic comments and the act of civic shaming is already widespread in both offline and online situations, and the arrival of unconstrained deep-fake technology will unavoidably exacerbate these problems. The necessity for private recordings has reduced due to the luxury with which individuals can formulate and allocate adult content highlighting others as a means of seeking reckoning, either among associates or within online social webs.

Some of the content generated is extremely deceptive which ignites partial consequences.[18] In

[15] China Law Vision,
Deep Synthesis (Not Deepfake): How AI Compliance Works in China, https://www.chinalawvision.com/2025/02/digital-economy-ai/deep-synthesis-not-deepfake-how-ai-compliance-works-in-china/ (last visited Mar. 18, 2025).

[16] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, INDIA GAZETTE,
https://egazette.gov.in/WriteReadData/2023/248045.pdf (last visited Mar. 18, 2025).

[17] gdpr.eu, What is GDPR, the EU General Data Protection Regulation?
, https://gdpr.eu/what-is-gdpr/ (last visited Mar. 18, 2025).

[18] Combatting Deep-fakes in India - An Analysis of the Evolving Legal Paradigm and Its Challenges, 15 Int'l J.L. & Legal Stud. 287 (2024), https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/ijlj15&section=22

spite of the cognizance among those persons that the explicit content in enquiry is a wrought digital depiction, the latent penalties on society can be penetratingly unfavorable. These happenings are utter negative to a person's sense of self and self-esteem, and any post-facto redressal will not be able to reimburse solely for such forfeiture.

V. MITIGATING THE RISKS OF DEEP-FAKE TECHNOLOGY: A MULTILAYERED APPROACH TO ETHICS, LAW, AND DIGITAL LITERACY

Bearing in mind the consequences and problems accessible by deep-fake technology underlines how immediately this unruly needs to be fixed. It asks for a multilayered policy that comprises operator schooling, moral contemplation, lawful agendas, technical advances, and obliging exertions to assurance the accountable use of deep-fake technology and defense the truthfulness of digital media.[19] The fallout support the recommendations for additional study, the preparation of strategy, and the expansion of technology:

1. Lawmakers need to create comprehensive legal frameworks that address the making, sharing, and malevolent use of deep-fakes. Therefore, these entails considerations for regulating governing consent, intellectual property, privacy rights, and the proper use of deep-fake technology. Clear and implemented laws will provide legal remedies for those impacted by deep-fakes as well as a deterrent.
2. Educational initiatives should be developed to enhance users' media and digital literacy. This entails teaching individuals how to evaluate information critically, recognize deception, and verify the accuracy of media content. Users with the necessary skills can traverse the digital landscape more skillfully and reach educated decisions.
3. Promote moral principles and responsible conduct among individuals who create and use deep-fake technology. Emphasize how important it is to obtain consent, respect people's right to privacy, and limit the use of deep-fake technology to legitimate, non-nefarious purposes. Public awareness campaigns can be quite successful in highlighting the ethical concerns and appropriate the use of deep-fake technologies.
4. Provide financial support for the research and development of deep-fake detecting technologies. Governments, tech companies, and educational institutions can collaborate to create and enhance deep-fake detection systems.

(last visited Mar. 18, 2025).

[19] (PDF) Artificial Intelligence in digital media: The Era of Deepfakes, https://www.researchgate.net/publication/342795647_Artificial_Intelligence_in_Digital_Media_The_Era_of_Deepfakes (last visited Mar 18, 2025)

VI. CONCLUSION: A DIGITAL EPIDEMIC NEEDS AN URGENT RESPONSE

The Bhartiya Nyaya Sanhita (BNS), 2023 despite covering voyeurism, defamation and obscenity, still lacks specific provision for deep-fake pornography and in the age of AI-Driven deception, laws are still being drafted for conventional crimes completely ignoring technological exploitation. As Union Minister Rajeev Chandrasekhar rightly pointed out, "While AI is the buzzword and ChatGPT is fancy, we need legislative guardrails of safety and trust, which can ensure that AI can never be misused and or used by bad actors to cause harm."[20] This reality demands urgent intervention.

The need of the hour is a to strike the correct equation between innovation and protection. AI Should empower rather than exploiting the societal integrity and moral values. Without the enactment of robust legal and technological defenses, deep-fakes will continue to be a risk factor which will surely become a digital wildfire, destroying the reputations and lives of innocent at a drastically large scale.

*****

[20] Ai needs legislative guardrails of Safety, Trust: Rajeev Chandrasekhar The Economic Times, https://economictimes.indiatimes.com/tech/technology/ai-needs-legislative-guardrails-of-safety-trust-rajeev-chandrasekhar/articleshow/105635330.cms (last visited Mar 18, 2025)

 [ISSN 2581-5369]