ISSN: 3048-8702(O)

LLRJ

LEX LUMEN RESEARCH JOURNAL

VOLUME 2 - ISSUE 2

2025

EDITOR-IN-CHIEF: DR. RAZIT SHARMA,
PUBLISHER: MRS. RACHANA

LEX LUMEN RESEARCH JOURNAL-ISSN:3048-8702
Open Access, Double blind-Peer Reviewed Law Journal, Licensed by-CC BY-NC-SA.
Editor-in-Chief: Prof. (Dr). Razit Sharma, Publisher: Mrs. Rachana

Volume-2, Issue-2 ***Pages: 1-15***

UNDERSTANDING DEEPFAKE TECHNOLOGY, ITS MISUSE AND ADEQUACY OF LEGAL PROTECTIONS IN THE INDIAN CONTEXT

By- **Sainikitha.OL**[1]

ABSTRACT

Deepfakes videos and audios manipulated using artificial intelligence and other tools are no longer just a technological novelty but they are becoming a major serious threat to privacy, reputation, and even democracy in India. With millions of internet users, deepfakes can spread misinformation, influence voter's decisions in election, and target women and children in many harmful ways. This paper analyses how India's legal regime, such as the IT Act 2000, IT Rules 2021, Digital Personal Data Protection Act 2023, POCSO Act 2012, and Bharatiya Nyaya Sanhita 2024, try to withstand these harms in the absence of a standalone statute for deepfakes. It also examines various cases involving celebrities, politicians, and influencers to understand the multifaceted harms that are being caused by deepfakes. Regulatory bodies like MeitY, SAHYOG/I4C, and the Data Protection Board play an important and crucial role in monitoring, taking down harmful content, and protecting personal data of individuals, but their actions are often reactive than being proactive. The paper suggests the need for a dedicated deepfake law, clear rules on watermarking AI content, stronger accountability for platforms and intermediaries, steadfast remedies for victims, stricter election safeguard measures by ECI, and better public awareness via campaigns. Only by understanding legal, technical, and social

[1] Intern-Lex Lumen Research Journal.

Volume-2, Issue-2 *Pages: 1-15*

measures India can protect its citizens and its democracy from the rising threats posed by synthetic media.

KEYWORDS: Deepfakes, Synthetic Media, Electoral Integrity, Artificial Intelligence, Intermediary

INTRODUCTION:

Deepfakes are powered by artificial intelligence and are capable of creating hyper realistic fake videos and audio that can easily manipulate the reality, pose severe threats to India's democracy, privacy, and the very social fabric. As the world's largest democracy with over 850 million internet users, India grapples with deepfakes spreading unnecessary misinformation, manipulating electoral decisions and instigating gendered violences especially against women.[2]

Deepfake technology uses generative adversarial networks (GAN) to swap faces and mimic voices which makes such audios and videos hyper realistic. In India, its rise is strengthened by and with booming digital penetration, causing risks during elections and beyond. From Rashmika Mandanna's (an Indian actress) viral morphed video to political audio, deepfakes erode public trust and allows the perpetrators to easily commit privacy violations. Courts and other regulators such as MEITY and Data Protection Board now scramble to adapt to this new technology with the old enactments.[3] This paper examines India's legal responses, case studies, legal protections and needed reforms.

---

[2] *Deepfakes in India: Legal Landscape, Judicial Responses, and a Practical Playbook for Enforcement*, NEGD (Sept. 29, 2025), https://negd.gov.in/blog/deepfakes-in-india-legal-landscape-judicial-responses-and-a-practical-playbook-for-enforcement/.

[3] Akhilesh Sharma, *3 Years Jail, 1 Lakh Fine: Centre's Reminder After Actor Rashmika Mandanna Deepfake Row*, NDTV (Nov. 7, 2023, 8:11 PM IST), https://www.ndtv.com/india-news/centres-rule-reminder-to-social-media-sites-on-rashmika-mandanna-deepfake-4553378.

Volume-2, Issue-2 *Pages: 1-15*

OBJECTIVES OF THE STUDY:

This study aims to understand and analyse India's deepfake regulatory regime, scrutinize applicable laws, and assess their enforcement efficacy. It further evaluates how various provisions under the Information Technology Act, 2000, IT Rules 2021 and Digital Personal Data Protection Act 2023 withstand synthetic media without explicit statutes governing the deepfakes. Ultimately, it evaluates whether the current measures suffice amidst rising deepfake threats and privacy violations in the current digital realm.[4]

LEGAL PROVISIONS RELATING TO DEEPFAKE VIOLATIONS:

India lacks a standalone deepfake law. Yet, various statutes are currently being used to address the deepfake issue. It includes,

- **The Information Technology Act, 2000**

The Act u/s. 66D regulates and punishes cheating by impersonation using computer resource. The offence is punishable with both imprisonment and fine.[5] The section 66E further deals with violation of privacy.[6] The section 67 deals with punishment for publishing and transmitting obscene material in electronic format.[7] The act of publishing and transmitting sexually explicit contents in electronic forms are dealt u/s. 67A,[8] while s. 67B deals with child specific sexually explicit contents.[9] The above mentioned provisions are generally used and relied on when an offense is committed

[4] Chaksham Kumar Das, *Deepfakes and Indian Law: Is the IT Act Enough in the Age of AI?*, Century Law Firm, https://www.centurylawfirm.in/blog/deepfakes-and-indian-law-is-the-it-act-enough-in-the-age-of-ai/.
[5] Information Technology Act, No. 21 of 2000, § 66D.
[6] Id. § 66E.
[7] Id. § 67.
[8] Id. § 67A.
[9] Id. § 67B.

using the deepfake technology in the absence of separate statute. The central and state government is also empowered to decrypt and intercept certain contents online but with limited grounds to exercise the power. For e.g. Sovereignty and integrity of India, Defence of India and so on. u/s. 69 and 69A[10] of the Act.

- **The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021**

The section 3 of the Act particularly deals with Due Diligence whereby intermediaries including the social media intermediaries are mandated to follow certain mandates under the rules.[11] Especially, Rule 3(b)(ii) and (iii) deals with gender specific obscene and child specific harmful contents from being displaced. A Grievance Redressal Officer shall be appointed under the grievance redressal mechanism given u/s. 3(2).[12] This mechanism could also be extended specifically to include deepfake violations and harms. As per section 4(2) of the Rules, a significant social media intermediary shall enable the identification of the first originator of the information upon a judicial order.[13] This provision enables to find the initial publisher and thereby helps to trace down the perpetrator.

- **Digital Personal Data Protection Act, 2023**

The Act requires certain grounds for processing digital personal data of a data principal u/s. 4 of the Act.[14] It includes consent of the data principal and for legitimate use of data. A notice has to be sent by the data fiduciary u/s. 5 of the Act.[15] Also, the

[10] Id. §§ 69, 69A.
[11] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 3.
[12] Id. § 3(2); § 3(b)(ii)-(iii).
[13] Id. § 4(2).
[14] Digital Personal Data Protection Act, 2023, § 4.
[15] Id. § 5.

Volume-2, Issue-2 *Pages: 1-15*

data principal has a right of erasure of personal data u/s. 12 of the Act.[16] This allows a person to formally seek erasure of s of audio visual deepfake contents online.

- **The Protection of Children from Sexual Offences Act, 2012**

The Sections 13 to 15 of the POCSO Act punishes child pornographic contents and particularly section 15 of the Act punishes the act of storing child pornographic material.[17]

- **Bharatiya Nyaya Sanhita, 2024**

The act of spreading obscene material is punished u/s. 294 of the Sanhita.[18] However, the act of creating such content especially using deepfake content often remains unnoticed and hence, this loophole is often used by persons to create and spread harmful deepfake contents.

RELEVANT CASES AND INCIDENTS:

In Rashmika Mandanna's 2023 deepfake case, her face was swapped onto influencer Zara Patel's body. The Delhi Police arrested creator Eemani Naveen under IT Act Sections 66D and 67. Financial influencers Ankur Warikoo secured Delhi High Court injunction order in May 2025 against deepfake videos of him, harming his reputation by spreading fake investment advice videos of him. BJP politician Manoj Tiwari's multilingual deepfakes targeted Delhi voters and PM Modi went on to warn about the deepfakes issues in the contemporary era.

DEEPFAKES IN ELECTIONS:

[16] Id. § 12.
[17] Protection of Children from Sexual Offences Act, No. 32 of 2012, §§ 13–15.
[18] Bharatiya Nyaya Sanhita, 2023, § 294.

Volume-2, Issue-2 *Pages: 1-15*

Deepfakes manipulate voters' decisions in elections by fabricating various scandals. In India's 2024 Lok Sabha polls, parties generated millions of AI voice calls in 22 languages for voter outreach, but malicious clips like digitally cloned leaders inciting violence often spread unverified. ECI mandated 3-hour removal of fake contents online mandate.[19]

In the case of Rukumini Madegowda vs The State Election Commission & Ors,[20] the court stated that the Election Commission has wide powers under Article 324(1) to issue directions necessary for conducting free and fair elections, subject to the contours of law. The power of the Election Commission includes the power to issue directions where the law is silent. The powers of ECI are also executive in nature and thus, the Commission has the power to issue directions in cases of Deepfake violations particularly during the election period.

OFFENCES AGAINST WOMEN AND CHILDREN:

Deepfakes have emerged as a terrible harmful tool when used against women and children, turning technology into a tool of humiliation and coercion. Unlike traditional cybercrimes, deepfake abuse often leaves victims feeling powerless, as their own face or voice is used against them without due consent. In India, women form the largest group of victims of non-consensual deepfake pornography, where images are sourced from social media, manipulated into explicit content and circulated widely to threaten the women. Such acts not only violate privacy but also deeply affect dignity, mental health, and social standing of any women against whom deepfakes are deployed.[21]

---

[19] Anuradha Gandhi & Isha Sharma, *PIL and Election Commission of India's Response on Deepfakes*, S.S. Rana & Co. (May 9, 2024), https://ssrana.in/articles/pil-eci-response-deepfakes/.
[20] Rukmani Madegowda v. The State Election Commission & Ors, (2002) LiveLaw (SC) 766.
[21] NCRB, *Crime in India; Cyber Crime Statistics* (2020–2024); UNESCO, *Gendered Impacts of Deepfakes*.

Volume-2, Issue-2 *Pages: 1-15*

Children are even more vulnerable to offences connected with deepfakes. The emergence of virtual child sexual abuse material (child pornography), where a child's likeness is digitally created or altered, presents serious legal and moral concerns. Even in cases where no physical contact occurs, the harm to the child's dignity, safety, and psychological well-being is undeniably potent to be protected.

REGULATING BODIES:

1. MeitY (Ministry of Electronics and Information Technology)

MeitY is the central government ministry governing India's digital policies and other decisions including how the internet should be governed and how new technologies like AI are to be managed and regulated in India.

- Policy and advisories: MeitY has been pushing rules that force social media companies and tech platforms to actively monitor and manage deepfakes and synthetic content. It has issued formal advisories that urge and mandate platforms to clearly label AI generated material, stop harmful deepfake content from appearing in their platforms upon notice, and act quickly when issues are being reported.[22]
- Draft rule making: MeitY has proposed updates to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules to require platforms to verify user claims about synthetic content and mandate visible markers on such content so that users can tell if something is AI generated,

[22] Ojasvi Gupta, *Regulation soon to rein in deepfakes: Mandatory labelling, user declarations proposed*, Financial Express (Oct. 22, 2025), https://www.financialexpress.com/india-news/regulation-soon-to-rein-in-deepfakes/4018442/.

Volume-2, Issue-2 *Pages: 1-15*

allowing users to remain informed about the authenticity of the contents online.[23]

- Due diligence: Platforms that fail to take responsible action such as failing timely removal or labelling might risk losing the available legal protections under the IT Act, which normally shields them from liability for content generated by its users.[24] i.e. Safe Harbour.

In short, MeitY sets the regulatory advises and mandates, it defines what platforms must do against harmful deepfake contents, how they should treat them, and sets standards under Indian digital legal regime.

2. SAHYOG / I4C (Centralised Mechanism for removal under Cybercrime Framework)

SAHYOG is a portal which is managed by the Indian Cyber Crime Coordination Centre (I4C) under the Ministry of Home Affairs. SAHYOG isn't a standalone law-making body but rather a practical enforcement tool that helps the government to act on unlawful online content including deepfakes.

- Takedown notices: SAHYOG helps enforcement bodies and authorised agencies to quickly send legal takedown requests (mostly orders) to social

[23] Explanatory Note, *Proposed Amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 in relation to synthetically generated information* (Oct. 22, 2025), Ministry of Electronics & Information Technology (MeitY), https://www.meity.gov.in/static/uploads/2025/10/8e40cdd134cd92dd783a37556428c370.pdf.

[24] Ojasvi Gupta, *Regulation soon to rein in deepfakes: Mandatory labelling, user declarations proposed*, Financial Express (Oct. 22, 2025), https://www.financialexpress.com/india-news/regulation-soon-to-rein-in-deepfakes/4018442/. (financialexpress.com)

Volume-2, Issue-2 *Pages: 1-15*

media platforms. These requests require the company to remove or disable access to content that violates the law and rights of the citizens.[25]

- Centralised Process: Rather than requiring each and every police officers or agencies to manually write separate written or typed orders, SAHYOG centralises and tracks these notices, making enforcement faster and more structured, ensuring speedy redressal to the affected individuals.[26]

3. Data Protection Board (established under the recent Digital Personal Data Protection Act:

The Data Protection Board of India (also known as DPB) is an authority established under the Digital Personal Data Protection Act, 2023 to oversee compliance with personal data rights and to deal with data violations.

- Privacy and misuse of personal data: A lot of deepfake harm stems from unauthorised use of a person's face, voice, or other relevant personal data. The DPDP Act mandates that personal data must be processed only with the appropriate consent of the affected individual i.e. Data Principal as per the Act. If deepfakes misuse personal data especially data used without the person's consent, the DPB can adjudicate complaints and order remedies or penalties against the perpetrator or violator.
- Accountability for intermediaries: The Board evaluates whether companies or entities (data fiduciaries as per the Act) have followed prescribed data

[25] *India well-equipped to tackle evolving online harms and cybercrimes; Government to Parliament*, Press Information Bureau, Ministry of Electronics & IT (Aug. 8, 2025), https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2154268. (pib.gov.in).
[26] Sahyog Portal, Ministry of Home Affairs, Gov't of India, https://sahyog.mha.gov.in.

Volume-2, Issue-2 *Pages: 1-15*

protection norms, including preventing breaches that could lead to misuse in synthetic content.

- Enforcing data rights: Individuals harmed by deepfakes can potentially invoke data protection rights, such as erasure of their data or seek compensation before this Board. The penalty enforceable by the board extend up to 200 crore rupees for personal data violations.

RECOMMENDATIONS:

1. **Standalone Deepfake Law:**

   India immediately requires a dedicated legislation for the purpose of addressing deepfakes and their curated harms, rather than relying on the existing provisions under the IT Act, BNS, and other statutes. A standalone law should clearly define what is deepfake? and synthetic media, criminalise malicious creation using someone's personal data and dissemination of the violating content, and differentiate between permissible uses such as satire, parody, research and harmful misuse (child pornography, electoral manipulations and contents affecting modesty of a woman etc.,). This would reduce ambiguity in enforcement and ensure proportional penalties against the harm caused to the victims.[27]

2. **Mandatory Disclosure and Watermarking of AI Generated Deepfake Content:**

   All AI generated audio visual deepfake content should carry mandatory disclosures such as watermarks. Converting Meity's direction regarding

[27] Law Commission of India, *Emerging Challenges in Cyber Law and Artificial Intelligence* (Discussion Papers).

Volume-2, Issue-2 *Pages: 1-15*

watermarking contents into statutory obligation would enhance compliance and accountability among both platforms and individuals. This measure would empower users to identify such manipulated content and preserve their safety and dignity in the digital environment.[28]

3. **Strengthen Intermediary Accountability beyond Safe harbour:**

   The current 36-hour takedown mandate under the IT Rules should be supplemented with a response mechanism, allowing faster removal in crucial cases involving elections, sexual abuse, or child exploitation. At the same time, these safety measures must be immune to prevent arbitrary censorship which ensures compliance with Article 19(1)(a) of the Constitution protecting free speech and expression.[29]

4. **Expand the Mandate of SAHYOG / I4C:**

   SAHYOG should be evolved beyond a mere takedown facilitation portal into a specialised synthetic media response unit, supported with technical tools to identify deepfakes and coordinate with platforms in real time in a fast manner. The absence of tools to identify remain a major issue to almost the entire word. There is no 100% deepfake detector tool till date. Also, capacity building of police officials and cybercrime units at different levels is equally crucial to ensure victims receive timely redress without undue delays.[30]

5. **Extending the Data Protection Board's Jurisdiction to Harmful Deepfakes**: The DPDP Act should explicitly recognise deepfake based misuse of facial and

[28] MeitY Advisories on AI-Generated Content (2023–2025); Business Today Reports.

[29] *Shreya Singhal v. Union of India*, (2015) 5 SCC 1; IT Rules, 2021.

[30] Press Information Bureau, Government of India, SAHYOG Portal Releases.

voice data as a form of personal data violation rather than using indirect and vague terms and definitions.[31]

6. **Election and deepfakes:**

The Election Commission of India should issue binding guidelines prohibiting deceptive deepfake content during the election periods. Fast track grievance redressal mechanisms during the Model Code of Conduct period are essential to protect electoral integrity.[32] The Election Commission had issued notification regarding the wrongful use of deepfakes and the consequences thereof. Such constant reminder notification and warnings are essential to protect voters' autonomy, ultimately protecting the right to free and fair election and the democracy.

7. **Victim Centric Remedies and Psychological Support:**

The focus should drift from punishments and financial penalties to victim centric approach. Fast track courts for cyber sexual offences, access to counselling services, and anonymous complaint filing mechanisms should be institutionalised, particularly for women and children who are often the victims of such harmful contents available online.[33]

8. **Public Awareness and Digital Literacy Campaigns:**

Finally, the regulatory action must be complemented by public education and awareness about the pros and cons of deepfake technology. Government should organize digital literacy campaigns and must train the citizens to

[31] Digital Personal Data Protection Act, 2023.
[32] Election Commission of India, Model Code of Conduct Guidelines
[33] NCRB, *Cyber Crime in India* Reports; POCSO Act, 2012.

Volume-2, Issue-2 *Pages: 1-15*

identify manipulated deepfake content, verify sources, and report deepfakes to the appropriate authorities.[34]

CONCLUSION:

India's deepfake regime hinges mainly on adaptive laws like IT Act and BNS, yet these enforcements struggle to keep up with the fast-growing AI developments.[35] Deepfakes are no longer a distant or mere technical problem that can be taken simply. It affects people's rights, elections, and real lives.

Laws like the IT Act, the Bharatiya Nyaya Sanhita, and the data protection framework offer some protection, yet they were created before deepfakes became a common tool for harm. As a result, enforcement often feels reactive rather than preventive. Regulatory bodies such as MeitY, SAHYOG, and the Data Protection Board play an important role, but advisories and takedown orders alone cannot fully address reputational, and democratic harm that are caused by deepfakes.

Currently, stricter law is a need of the hour, however a clearer and balanced approach is required to address the harms and threats posed by this technology. Victims must have quick and effective remedies, platforms must take responsibility for what spreads on through their systems, and citizens must be equipped to question and verify what they see and listen online.

[34] UNESCO, *Guidance on AI and Information Integrity*; MeitY Digital Literacy Initiatives.

[35] *AI Generated Content Regulation in India*, Drishti IAS (Oct. 25, 2025), https://www.drishtiias.com/daily-updates/daily-news-editorials/ai-generated-content-regulation-in-india.

Volume-2, Issue-2 *Pages: 1-15*

REFERENCES:

1. **Sheikh Inam Ul Mansoor,** ***Legal Implications of Deepfake Technology: In the Context of Manipulation, Privacy, and Identity Theft*****, Central University of Kashmir Law Review, Vol. 4 (Dec. 2024),** https://www.researchgate.net/publication/387499036_Legal_Implications_of_Deepfake_Technology_In_the_Context_of_Manipulation_Privacy_and_Identity_Theft. (researchgate.net)
2. **Juhi Chandel & Manisha Kundu,** AI-Generated Deepfakes and the Legal Vacuum in India: A Constitutional Analysis of Privacy, Consent, and Digital Harm Under Article 21, 10 No. 11 Int'l Journal of Research in Technology and Innovation (IJRTI) 99 (Nov. 2025), https://ijrti.org/papers/IJRTI2511099.pdf.
3. **Karan Choudhary & Mahak Rajpal,** Criminalizing Deepfake Technology in India: A Legal Analysis of Privacy and Regulatory Gaps, 5 Int'l J. of Advanced Legal Research 3 (Feb. 2025), https://ijalr.in/wp-content/uploads/2025/04/CRIMINALIZING-DEEPFAKE-TECHNOLOGY-IN-INDIA-A-LEGAL-ANALYSIS-OF-PRIVACY-AND-REGULATORY-GAPS.pdf.
4. **Sathiyapriya R. K.,** Deepfakes and the Right to Privacy: Socio-Legal Challenges in India, 12 J. Emerging Technologies & Innovative Research (JETIR) 5 (May 2025), www.jetir.org **(ISSN 2349-5162).**
5. **Abhinandhan B.,** Legal Implications of Deepfake Technology: Privacy, Defamation, and Consent Research Project, 5 Indian J. of Legal Review (IJLR) 9 (2025), https://iledu.in.

6. **Aditya Mehrotra,** Dissecting the Framework of Deep Fakes in India – A Glaring Lacuna, Cell for Law & Technology, **National Law Institute University (Jan. 6, 2024),** https://clt.nliu.ac.in/?p=887. (clt.nliu.ac.in).

7. **Kuldeep Singh Panwar & Nilutpal Deb Roy,** Rising Menace of Deepfakes with the Help of AI: Legal Implications in India, 4 Indian J. of Integrated Research in Law (IJIRL) 3 (2024), https://ijirl.com/wp-content/uploads/2024/05/RISING-MENACE-OF-DEEPFAKES-WITH-THE-HELP-OF-AI-LEGAL-IMPLICATIONS-IN-INDIA.pdf.

8. **Rishita Yadav,** Navigating the Legal Landscape: Addressing Deepfake Concerns in India Through Enhanced Legislative Frameworks and Collaborative Strategies, 3 J. of Legal Research & Juridical Sciences 215 (2025), www.jlrjs.com **(ISSN 2583-0066).**