INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA).*

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

REGULATING DEEPFAKES: EMERGING FORMS OF CYBERCRIME AND THE ADEQUACY OF INDIAN CYBER LAWS

AUTHORED BY - DIVYANSHU KRISHNA
B.A. LL.B., Second Year

CO-AUTHOR - ABHAY SINGH,
B.Tech (CSE–AI), Final Year

Abstract

Deepfake technology uses advanced artificial intelligence models to generate highly realistic synthetic audio-visual content that can convincingly imitate a person's face, voice, and mannerisms, often without consent.[4] In India, deepfakes have already been deployed for political manipulation, financial frauds, and non-consensual sexual content, raising serious concerns about privacy, dignity, electoral integrity, and cyber security.[5] This doctrinal paper examines whether the existing Indian legal framework—principally the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023, and allied provisions—adequately addresses deepfake-based cybercrimes or whether more specific legislation is needed.[6] Analysing statutes, subordinate legislation, recent case law, and policy documents, the paper argues that India currently relies on a patchwork of offences and intermediary obligations that, while flexible, suffer from gaps in definition, victim-centric remedies, cross-border enforcement, and evidentiary standards, requiring targeted reform.[7]

I. Introduction

Deepfakes are synthetic images, videos, and audio produced by deep-learning systems that can closely mimic real individuals, thereby eroding the traditional distinction between authentic and fabricated media.[8] Advances in deep-learning architectures, especially Generative Adversarial Networks, have enabled the generation of hyper-realistic content that can deceive ordinary viewers.[9] This has profound implications for trust in digital communication, the probative value of audiovisual evidence, and the integrity of public discourse.[10]

ISSN: 2582-6433

India, with more than 850 million internet users and a rapidly expanding digital ecosystem, faces acute risks from deepfakes.[11] Media reports and policy analyses describe an emerging crisis in which AI-generated synthetic media is used to manipulate elections, deceive investors, harass women, and undermine public trust.[12] Instances include investment scams driven by deepfake videos of celebrated industrialists and obscene AI-generated content targeting film actors, which have prompted criminal complaints and urgent judicial intervention.[13] Commentators characterise India's deepfake challenge as one of both scale and urgency, noting that the proliferation and virality of such content outpace the ability of individuals and institutions to respond.[14]

In response, Indian institutions have begun to react. On the judicial side, high courts have issued wide-ranging injunctions to protect personality rights and privacy against deepfake misuse, including "John Doe" and dynamic orders directed at anonymous infringers and platforms.[15] On the regulatory side, the Ministry of Electronics and Information Technology (MeitY) has proposed and notified amendments to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, introducing an explicit framework for "synthetically generated information," mandatory labelling, and time-bound takedowns.[16] Academic writing has also proliferated, examining deepfakes from the perspectives of privacy, data protection, criminal liability, and human rights.[17]

The core research question in this paper is whether the current Indian cyber law framework adequately regulates deepfakes as a form of cybercrime, or whether a specialised statutory regime is required.[18] The methodology is purely doctrinal, relying on analysis of statutes, case law, government documents, and scholarly commentary; it does not include empirical surveys or technical experiments.[19]

II. Deepfake Technology and Harms

A. Nature and operation of deepfakes

Deepfakes are typically generated by training neural networks on large datasets of images, video frames, or audio clips depicting a target individual.[20] Through repeated training cycles, the model learns to reproduce the target's facial features, expressions, and voice patterns, ultimately producing synthetic media that appears authentic.[21] In a standard GAN framework, a generator attempts to create plausible synthetic outputs, while a discriminator tries to distinguish synthetic from real data, and both networks improve iteratively.[22]

ISSN: 2582-6433

From a legal perspective, the crucial point is that deepfakes often rely on personal data—especially facial images and voice samples—collected from publicly accessible sources such as social-media profiles, news footage, and video-sharing platforms.[23] Because such data are widely available, malicious actors can generate convincing deepfakes without any meaningful consent or direct hacking of secure systems.[24] The tools required to do so have become increasingly accessible; user-friendly applications and open-source software now allow non-experts to produce face-swapped videos and voice clones, lowering the barrier for abuse.[25]

B. Types of harms in the Indian context

Policy reports and media coverage in India identify at least four major categories of deepfake harms.[26]

First, deepfakes facilitate **political and electoral manipulation**. Synthetic videos can depict political leaders making inflammatory statements, endorsing particular parties, or speaking languages they do not command, thereby misleading voters and amplifying misinformation in the run-up to elections.[27] With messaging platforms and social media serving as primary channels for political communication, such content can spread rapidly and is difficult to debunk in real time.[28]

Second, deepfakes enable **financial and corporate frauds**. In one widely reported incident, Bengaluru residents were duped of nearly ₹95 lakh after being induced by deepfake videos of well-known corporate figures promoting fraudulent investment schemes.[29] These scams often exploit the perceived credibility of respected personalities, combining deepfake videos with WhatsApp groups and online platforms to solicit funds.[30]

Third, deepfakes inflict serious **sexual and gender-based harms**, particularly through non-consensual sexual deepfakes and obscene morphing of images.[31] Women, including actors and influencers, are disproportionately targeted, resulting in violations of privacy, dignity, and bodily autonomy.[32] A notable example is the registration of a criminal case concerning obscene AI-generated deepfake videos of a prominent Telugu actor, where police invoked provisions dealing with obscenity and cybercrime.[33]

Fourth, deepfakes can cause **reputational and social harms** by depicting individuals engaging in unlawful or immoral conduct, or endorsing views they do not hold, leading to social

ISSN: 2582-6433

ostracism and professional consequences even after the content is exposed as fake.[34] Commentators also warn of systemic harms: as deepfakes become more common, genuine audiovisual evidence may be dismissed as fabricated, undermining public trust and legal fact-finding.[35]

These harms demonstrate that deepfakes are not a mere technological curiosity but a significant challenge to criminal law, data protection, intermediary regulation, and constitutional rights.[36]

III. Indian Legal Framework

A. Information Technology Act, 2000 and IT Rules

The Information Technology Act, 2000 (IT Act) is the foundational statute governing cyber offences in India and, although enacted before the emergence of deepfakes, contains provisions that can be applied to many deepfake-based harms.[37] Section 66C criminalises identity theft through fraudulent use of another person's electronic signature, password, or other unique identification feature, and can be invoked against deepfakes that misappropriate identity markers.[38] Section 66D penalises cheating by personation using a computer resource, directly relevant where deepfakes are used in investment scams or impersonation schemes.[39] Section 66E deals with violation of privacy through capturing, publishing, or transmitting images of a person's private areas without consent, potentially covering intimate deepfake content.[40] Additionally, sections 67 and 67A prohibit the publication or transmission of obscene or sexually explicit material in electronic form, provisions that have long been applied in cases involving morphed images and non-consensual pornography and can likewise extend to sexual deepfakes.[41]

The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, impose **due-diligence obligations** on intermediaries, including requirements to take down unlawful content upon receiving actual knowledge—through court orders or government notices—of its illegality.[42] In October 2025, MeitY announced amendments that, for the first time, expressly addressed deepfakes and other "synthetically generated information."[43] These amendments introduce a definition of synthetic content, mandate labelling of AI-generated media, and require significant social-media intermediaries to remove harmful deepfakes within strict timelines (often 36 hours) upon receiving appropriate complaints or orders.[44] The amendments also place obligations on AI tool providers and clarify that good-faith takedowns of suspected deepfake content will not ordinarily attract liability.[45]

ISSN: 2582-6433

B. Bharatiya Nyaya Sanhita, 2023

The Bharatiya Nyaya Sanhita, 2023 (BNS), which replaces the Indian Penal Code, modernises several offence categories in ways that intersect with deepfake-related misconduct.[46] Key provisions include section 336 on cheating by personation; section 353 on statements conducing to public mischief; and sections 111, 319, and 356 addressing organised crime, personation, and forgery.[47] Commentators note that these provisions, when read together, enable prosecution of a wide variety of deepfake scenarios: financial scams using synthetic media can be addressed through cheating-by-personation provisions; communal or inflammatory deepfakes can be pursued under public-mischief provisions; and coordinated deepfake campaigns may fall within the ambit of organised cybercrime.[48]

However, the BNS does not contain an explicit statutory definition of deepfakes or synthetic media.[49] Instead, it relies on technology-neutral concepts such as personation, forgery, and statements causing public mischief.[50] While such flexibility is useful, the absence of explicit definitions may lead to inconsistent application and uncertainty, particularly for novel fact patterns that do not neatly fit existing categories.[51]

C. Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDPA) introduces a modern framework for the processing of personal data, including biometric identifiers such as facial images and voice samples that are often used to train and deploy deepfake models.[52] Deepfake generation that involves processing such data without valid consent or other lawful ground can constitute a breach of the DPDPA, potentially attracting substantial administrative fines—up to ₹250 crore for serious violations.[53] Data fiduciaries are required to process data lawfully, fairly, and only for specified purposes, implying that indiscriminate scraping and use of biometric data for deepfake creation may be unlawful.[54]

The DPDPA thus complements criminal-law provisions by regulating the **input side** of deepfakes—data collection and processing—rather than only the output.[55] Nevertheless, because DPDPA penalties are administrative and focus on data fiduciaries rather than individual offenders, it does not directly substitute for criminal sanctions in cases of malicious deepfake-based cybercrime.[56]

ISSN: 2582-6433

D. Other applicable laws and doctrines

Deepfakes also intersect with other statutes and doctrines. The Indecent Representation of Women (Prohibition) Act provides an additional statutory basis for addressing sexually explicit deepfakes targeting women.[57] Personality and publicity rights, recognised in Indian case law, protect individuals against unauthorised commercial exploitation of their name, image, and likeness, and have been invoked in suits challenging deepfake misuse of celebrity identities.[58] Constitutional protections under Article 21—including privacy, dignity, and reputation—provide a rights-based foundation for judicial remedies such as injunctions, damages, and directions to intermediaries.[59]

IV. Adequacy of the Current Framework

The existing framework exhibits several strengths. The combination of IT Act offences, BNS provisions, sectoral statutes, and DPDPA obligations allows prosecutors and regulators to address many deepfake scenarios without waiting for new primary legislation.[60] Intermediary rules provide a channel for swift removal of harmful content once notified, while recent amendments show that regulators are willing to update subordinate legislation to respond to AI-related risks.[61] Judicial creativity in granting dynamic and John Doe injunctions further strengthens protection for personality rights and privacy.[62]

However, doctrinal and practical gaps remain. The absence of a clear, technology-specific definition of deepfakes in primary legislation creates interpretive uncertainty and may hinder consistent enforcement across jurisdictions.[63] Victim-centric remedies are underdeveloped; existing rules do not yet guarantee uniform, user-friendly procedures for rapid takedowns, restoration of reputation, and structured compensation tailored to deepfake harms.[64] Cross-border enforcement poses continuing difficulties because deepfake content is often generated or hosted abroad, while mutual legal assistance and international cooperation remain slow.[65]

Deepfakes also pose novel evidentiary challenges. Scholars point out that deepfakes threaten both the authenticity and the perceived reliability of digital evidence, raising issues for admissibility under the emerging Bharatiya Sakshya Adhiniyam and related procedural frameworks.[66] Without robust forensic standards, technical capacity, and judicial guidance, courts may struggle to determine whether a contested video is authentic or synthetic, which affects both the prosecution of deepfake offences and the risk of false defences.[67]

ISSN: 2582-6433

V. Findings and Doctrinal Recommendations

Doctrinally, the Indian response to deepfakes can be characterised as a **functional patchwork**. Existing statutes can be interpreted to cover many harmful uses of deepfakes, particularly in relation to identity theft, cheating by personation, obscene and intimate synthetic content, and public-order threats.[68] Yet this flexibility comes at the cost of clarity, predictability, and victim-centric design.[69]

This paper therefore recommends:

- incorporation of a targeted statutory definition of deepfakes and "synthetically generated information" in primary legislation, with graded offences based on harm;[70]
- codification of clear, time-bound notice-and-action procedures and rights for victims seeking takedown and redress;[71]
- development of detailed forensic and evidentiary standards for deepfake detection, preservation,
- and admissibility, supported by specialised training;[72] and
- closer integration between deepfake-specific norms and the DPDPA, ensuring that unlawful biometric data processing is treated as a serious, aggravating factor.[73]

Such reforms would move Indian cyber law from a reactive, patchwork approach toward a more coherent, anticipatory framework capable of addressing deepfakes as a distinct, evolving category of cybercrime.[74]

Case Law Section (Post-Research-Paper)

This section, which you can place **after the main 6 pages**, briefly extracts and analyses key Indian decisions relevant to deepfakes, with Bluebook-style citations.[75]

1. Shilpa Shetty v. Getoutlive & Ors. (Bombay High Court, 2025)

In Shilpa Shetty v. Getoutlive & Ors., the Bombay High Court considered an application by actor Shilpa Shetty seeking interim protection against AI-generated deepfake images and videos portraying her in a pornographic and degrading manner.[76] The Court described the material as "extremely disturbing and abhorrent," held that such content violated her fundamental right to privacy and dignity under Article 21, and ordered the immediate takedown of all URLs hosting the deepfake material.[77] It further directed platforms to remove infringing content and emphasised that no person, "much less a woman," could be portrayed in this

ISSN: 2582-6433

manner without knowledge or consent.[78]

Citation (illustrative Bluebook form):

Shilpa Shetty v. Getoutlive & Ors., Interim Order (Bom. HC Dec. 25, 2025), summarized in High Court Orders Takedown of AI Deepfakes of Shilpa Shetty, INDIA TODAY (Dec. 25, 2025), https://www.indiatoday.in/india/law-news/story/bombay-high-court-orders-takedown-ai-deepfakes- shilpa-shetty-2842151-2025-12-26.[79][1][2]

2. Ankur Warikoo v. Unknown Persons & X Corp. (Delhi High Court, 2025)

In a suit filed by entrepreneur-influencer Ankur Warikoo, the Delhi High Court granted a John Doe, ex parte ad interim injunction restraining unknown persons from creating or circulating deepfake videos misusing his name, image, voice, or persona to promote fraudulent investment schemes.[80] The Court directed the platform (defendant No. 2) to take down the infringing deepfake content within 36 hours of notice and to disclose details such as IP addresses, URLs, and account information related to the offending content.[81] Recognising the potential for serious reputational harm and financial loss, the Court held that a prima facie case existed and that the balance of convenience favoured the plaintiff.[82]

Citation (illustrative Bluebook form):

Ankur Warikoo v. Unknown Persons & X Corp., CS (Comm) No. _of 2025 (Del. HC May 28, 2025), summarized in Delhi High Court Passes John Doe Order Restraining Deepfake Videos, LIVE LAW (June 1, 2025), https://www.livelaw.in/high-court/delhi-high-court/delhi-high-court-ankur-warikoo-deepfake- videos-restrained-293539.[83][3][4][5]

3. Chiranjeevi Deepfake Obscenity Case (Hyderabad Police, 2025)

In October 2025, a criminal case was registered after AI-generated obscene deepfake videos of actor Chiranjeevi surfaced online.[84] According to reports, Hyderabad cyber-crime authorities invoked provisions of the IT Act and obscenity laws to investigate and remove the content.[85] The matter illustrates law-enforcement's willingness to treat deepfake production and dissemination as falling within existing cybercrime and obscenity frameworks, even in the absence of a specific deepfake offence.[86]

Citation (illustrative Bluebook form):

Case Filed Over AI-generated Obscene Deepfake Videos of Telugu Actor Chiranjeevi, NDTV

ISSN: 2582-6433

(Oct. 26, 2025), https://www.ndtv.com/india-news/case-filed-over-ai-generated-obscene-deepfake-videos-of-telugu- actor-chiranjeevi-9525054.[87][6]

Sample Footnotes (Bluebook Style, Shortened)

a. See Deepfakes in India: Legal Landscape, Judicial Responses and a Practical Playbook for Enforcement, NEGD (Sept. 28, 2025), https://negd.gov.in/blog/deepfakes-in-india-legal-landscape- judicial-responses-and-a-practical-playbook-for-enforcement.[7]

b. See Deepfake Regulation India 2025: MeitY's Comprehensive IT Rules Amendment, KHURANA & KHURANA (Dec. 15, 2025), https://www.khuranaandkhurana.com/deepfake-regulation-india- 2025-meity-s-comprehensive-it-rules-amendment.[8]

c. See Deepfake Evidence and the Indian Criminal Justice System: Challenges of Authenticity, Consent, and Admissibility in Law, IJFMR (Nov. 11, 2025), https://www.ijfmr.com/research- paper.php?id=60298.[9]

d. See Deepfake – How Real Is It?, KPMG (2024), https://assets.kpmg.com/content/dam/kpmgsites/in/pdf/2024/12/deepfake-how-real-is-it.pdf.[10]

e. See NEGD, supra note 1, at 4–7.[7]

f. See Information Technology Act, No. 21 of 2000, INDIA CODE; Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, INDIA CODE; Digital Personal Data Protection Act, No. 22 of 2023, INDIA CODE.[11][8]

g. See NEGD, supra note 1; IJFMR, supra note 3.[9][7]

h. See India's Evolving Legal Battle Against Deepfake Technology, SCRIPTED (2025).[12]

i. See KPMG, supra note 4, at 3–5.[10]

j. See SCRIPTED, supra note 8, at 2–4.[12]

k. See NEGD, supra note 1, at 3.[7]

l. See id.; Unmasking Deepfakes: Legal Risks and Remedies in India & Beyond, GNS LEGAL (Aug. 6, 2025).[13]

m. See Bengaluru Residents Duped of Rs 95 Lakh by Deepfake Videos of Narayana Murthy, TIMES OF INDIA TECH (Nov. 4, 2024); Case Filed Over AI-generated

ISSN: 2582-6433

Obscene Deepfake Videos of Telugu Actor Chiranjeevi, NDTV (Oct. 26, 2025).[14][6]

n. See India's Deepfake Problem: Scale and Urgency, HINDUSTAN TIMES (Dec. 11, 2025); Not Just

2. Money, Deepfakes Robbing People of Dignity, TIMES OF INDIA (Nov. 24, 2025).[15][16]

a. See Bom HC on Shilpa Shetty's AI-generated Deepfake Content, SCC ONLINE (Dec. 28, 2025); Delhi HC Grants John Doe Injunction to Ankur Warikoo, SCC ONLINE (May 28, 2025).[17][3]

b. See KHURANA & KHURANA, supra note 2; India Advances Deepfake Regulation with New IT Rules Amendment, AICERTS (Nov. 5, 2025).[18][8]

c. See, e.g., Regulating Deepfakes in India: A Legal and Ethical Analysis of Misinformation in the Age of AI, IJLLR (July 9, 2025); Chasing Deepfakes Across Borders & Protecting Rights, SCC ONLINE BLOG (Nov. 7, 2025).[19][20]

d. See NEGD, supra note 1, at 4–6.[7]

e. See IJFMR, supra note 3.[9]

You can now paste this into Word, set 12-pt Times New Roman, 1.5 or double spacing, and expand each section (especially Parts II–V and the case-law section) until it covers your required 6+ pages and beyond.

1. https://www.indiatoday.in/india/law-news/story/bombay-high-court-orders-takedown-ai-deepfakes-shilpa- shetty-2842151-2025-12-26
2. https://www.verdictum.in/court-updates/high-courts/bombay-high-court/shilpa-shetty-kundra-v-getoutlivein-personality-rights-privacy-violations-relief-removal-ai-deepfake-content-1602564
3. https://www.scconline.com/blog/post/2025/05/29/delhi-high-court-ankur-warikoo-john-doe-injunction-deepfake-ai-misuse-legal-news/
4. https://www.livelaw.in/high-court/delhi-high-court/delhi-high-court-ankur-warikoo-deepfake-videos-restrained-293539
5. https://www.lawfultalks.net/news/do-epic-shit-not-deepfake-scams-delhi-hc-issues-injunction-against-deepfakes- impersonating-ankur-warikoo
6. https://www.ndtv.com/india-news/case-filed-over-ai-generated-obscene-deepfake-videos-of-telugu-actor- chiranjeevi-9525054

ISSN: 2582-6433

7. https://negd.gov.in/blog/deepfakes-in-india-legal-landscape-judicial-responses-and-a-practical-playbook-for-enforcement/
8. https://www.khuranaandkhurana.com/deepfake-regulation-india-2025-meity-s-comprehensive-it-rules-amendment
9. https://www.ijfmr.com/papers/2025/6/60298.pdf
10. https://assets.kpmg.com/content/dam/kpmgsites/in/pdf/2024/12/deepfake-how-real-is-it.pdf
11. https://www.vifindia.org/article/2025/april/28/Bharatiya-Laws-Against-Deepfake-Cybercrime-Opportunities-and-Challenges
12. https://journals.ed.ac.uk/script-ed/article/download/12004/14850/42622
13. https://www.gnslegal.in/unmasking-deepfakes-legal-risks-and-remedies-in-india-beyond/
14. https://timesofindia.indiatimes.com/technology/tech-news/bengaluru-residents-duped-of-rs-95-lakh-by-deepfake-videos-of-narayana-murthy-and-mukesh-ambani/articleshow/114955868.cms
15. https://www.hindustantimes.com/ht-insight/future-tech/indias-deepfake-problem-scale-and-urgency-101765425799860.html
16. https://timesofindia.indiatimes.com/india/not-just-money-deepfakes-robbing-people-of-dignity/articleshow/125563834.cms
17. https://www.scconline.com/blog/post/2025/12/29/bom-hc-shilpa-ai-generated-deepfake-content-scc-times/
18. https://www.aicerts.ai/news/india-advances-deepfake-regulation-with-new-it-rules-amendment/
19. https://www.scconline.com/blog/post/2025/11/08/deepfake-regulation-rights/
20. https://www.ijllr.com/post/regulating-deepfakes-in-india-a-legal-and-ethical-analysis-of-misinformation-in-the-age-of-ai
21. https://www.thehindu.com/news/cities/mumbai/shilpa-shetty-moves-bombay-high-court-against-ai-deepfakes-and-misuse-of-her-identity/article70330207.ece
22. http://www.lawfultalks.net/news/do-epic-shit-not-deepfake-scams-delhi-hc-issues-injunction-against-deepfakes-impersonating-ankur-warikoo
23. https://sansad.in/getFile/BillsTexts/RSBillTexts/Asintroduced/2e214202543549PM.pdf
24. https://www.ptcnews.tv/nation/shilpa-shetty-deepfake-case-bombay-high-court-orders-removal-4419116
25. https://ijirl.com/wp-content/uploads/2025/06/NAVIGATING-DEEPFAKES-IN-

ISSN: 2582-6433

INDIAN-CRIMINAL-LAW-NAVIGATING-EVIDENTIARY-AND-LEGAL-REFORMS-UNDER-THE-BSA-AND-BNS-2023.pdf

26. https://www.wipo.int/wipolex/en/text/596125
27. https://juriscentre.com/2025/07/27/legal-dimensions-of-deepfake-technology-privacy-consent-and-criminal-liability/