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.

Copyright © International Journal for Legal Research & Analysis. All rights reserved.

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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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

THE DEEPFAKE DILEMMA: A DOCTRINAL ANALYSIS OF LEGAL REMEDIES AGAINST DEEPFAKE-BASED DEFAMATION AND HARASSMENT IN INDIA

AUTHORED BY - PUVIYA KEERTHI THIYAGARAJAN

Abstract

Deepfakes are synthetic audio, images and videos generated or altered by artificial intelligence so that they convincingly show a person doing or saying something that never happened. As the tools have become cheap and widely available, deepfakes have moved from novelty to a tool of reputational attack, sexual exploitation, fraud and harassment. India has no single statute on deepfakes. Victims must rely on the law of defamation, provisions of the Bharatiya Nyaya Sanhita, 2023, the Information Technology Act, 2000 and its Rules, copyright law, and the judge-made doctrine of personality rights. This paper analyses these remedies doctrinally, examines the recent trend of High Court injunctions against deepfakes, and evaluates the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, which for the first time regulate "synthetically generated information". It argues that the present framework is reactive, celebrity-centred and fragmented, and that ordinary victims, particularly women targeted by sexual deepfakes, are poorly served. The doctrinal analysis is supplemented by a public-opinion survey on awareness and attitudes. The paper closes with recommendations for statutory reform, platform accountability and victim-centred remedies.

Keywords: deepfakes, defamation, online harassment, personality rights, intermediary liability, synthetically generated information, IT Rules 2026

Introduction

The phrase "seeing is believing" no longer describes how people should treat digital media. Generative AI can now clone a voice from a few seconds of audio and place a person's face on another body with little technical skill. The legal difficulty is that the harm is real while the statement is false in a new way: there is no true statement that has been distorted, but an entirely fabricated event presented as evidence.

ISSN: 2582-6433

Two categories of harm dominate. The first is reputational: a fabricated video of a politician, professional or private person making offensive remarks, or an AI-generated endorsement of a fraudulent product. The second is harassment, including non-consensual sexual imagery, blackmail, impersonation and targeted abuse. Both harms spread quickly, are difficult to remove completely, and often originate from anonymous accounts or from platforms outside India.

The Indian response has so far come mainly from the courts. Since 2023, the Delhi and Bombay High Courts have granted numerous interim injunctions protecting the personality rights of public figures against AI misuse. In February 2026 the executive added a regulatory layer by amending the IT Rules. This paper asks whether these remedies, taken together, adequately protect victims.

Statement of the Problem

`Existing Indian law was drafted before generative AI. Defamation law presumes a "statement" attributable to a speaker, while deepfakes involve fabricated depictions. Criminal provisions on obscenity and identity theft apply only by analogy. Personality-rights jurisprudence, the most active area, protects chiefly those with commercial value in their persona. The result is uncertainty about which remedy applies, who is liable, and how quickly relief can be obtained.

Research Objectives

1. To examine the nature of deepfakes and the harms of defamation and harassment they cause.
2. To analyse the statutory and common-law remedies available in India.
3. To evaluate recent judicial trends and the 2026 amendment to the IT Rules.
4. To assess public awareness of, and attitudes towards, deepfake regulation through a survey.
5. To suggest reforms to close identified gaps.

Research Questions

1. Do existing Indian laws adequately address defamation and harassment caused by deepfakes?
2. How have Indian courts adapted personality rights and defamation law to deepfakes?

ISSN: 2582-6433

3. What is the effect of the IT Rules amendment of 2026 on platform liability and victim remedies?
4. What does public opinion indicate about awareness and the perceived adequacy of the law?

Hypotheses

H1: The existing legal framework is fragmented and reactive, and does not adequately protect ordinary victims of deepfakes.

H2: Most members of the public are aware of deepfakes but consider current laws inadequate.

Research Methodology

This study is primarily doctrinal. It analyses primary sources (statutes, rules, notifications and judicial decisions) and secondary sources (books, journal articles, reports and legal commentary) to identify, interpret and critique the law. A limited non-doctrinal component complements this analysis: a structured questionnaire administered through an online form to [number] respondents selected by [convenience / purposive] sampling, covering awareness of deepfakes, experience of harm, adequacy of law and preferred allocation of liability. Responses are presented as percentages in pie charts. Limitations: the sample is [small / non-random], so the findings are indicative and cannot be generalised to the whole population. Court orders discussed are mostly interim and may have been modified or made final since the date of writing.

Understanding Deepfakes

The term combines "deep learning" and "fake". Technically, deepfakes are produced using generative adversarial networks and related models in which one system generates content and another tries to detect it, so quality improves iteratively. Common forms include face-swapping, lip-syncing, voice cloning and fully synthetic persons. Chesney and Citron identify harms to individuals, such as exploitation and sabotage, alongside harms to institutions and democratic discourse, and note the "liar's dividend", where genuine evidence can be dismissed as fake.

The 2026 IT Rules adopt the label "synthetically generated information" (SGI), defined as audio, visual or audio-visual information that is artificially or algorithmically created or altered so that it appears real. Text-only content is outside this definition.

ISSN: 2582-6433

Legal Framework in India

Constitutional foundations

The right to privacy, including dignity and control over personal identity, flows from Article 21 as recognised in K.S. Puttaswamy v. Union of India (2017) 10 SCC 1. Counterbalancing it is freedom of speech under Article 19(1)(a), which, as explained in Shreya Singhal v. Union of India (2015) 5 SCC 1, can be restricted only on the grounds in Article 19(2) and through clear, narrowly framed rules. Reputation is part of Article 21, a position used in Subramanian Swamy v. Union of India (2016) 7 SCC 221 to uphold criminal defamation.

Defamation

Criminal defamation is dealt with in section 356 of the Bharatiya Nyaya Sanhita, 2023 (BNS), which replaced section 499 of the Indian Penal Code, and civil defamation proceeds as a tort for damages and injunction. A deepfake showing a person making false or derogatory statements fits comfortably within the idea of imputation harming reputation, as the representation is made by visual or audio means. Difficulties arise in attribution, proof of publication by anonymous users, jurisdiction, and the defences of truth, good faith and fair comment, which are hard to apply to wholly fabricated media. Remedies are also slow relative to the speed of online spread.

Harassment and sexual exploitation

Several BNS provisions are relevant to deepfake harassment: sexual harassment (s.75), voyeurism (s.77), stalking (s.78), forgery for the purpose of harming reputation (s.336), criminal intimidation (s.351) and statements conducing to public mischief (s.353). Under the Information Technology Act, 2000, section 66C (identity theft), section 66D (cheating by personation using a computer resource), section 66E (violation of privacy), sections 67, 67A and 67B (obscene, sexually explicit and child sexual abuse material) and section 69A (blocking of public access) are commonly invoked. Section 79 grants intermediaries safe harbour subject to due diligence and expeditious removal on notice. A major gap is that these provisions were not written with synthetic sexual imagery in mind, and prosecution depends on identifying the creator.

Copyright and moral rights

The Copyright Act, 1957 gives performers rights under section 38 and moral rights under section 57. These can support claims where a performer's voice or performance is cloned, but

ISSN: 2582-6433

they do not protect everyone whose likeness is used, and they do not directly address non-commercial reputational harm.

Personality and publicity rights

Indian courts have developed personality rights from privacy and passing-off principles. The Delhi High Court's decision in DM Entertainment Pvt. Ltd. v. Baby Gift House (2010) is a key early authority. Courts now treat name, image, voice and likeness as protectable attributes, and have extended these to AI avatars and voice clones.

Data protection

The Digital Personal Data Protection Act, 2023 regulates processing of personal data and may support claims where images or voice are processed without consent. Its practical value against anonymous deepfake creators is limited.

The IT Rules Amendment, 2026

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 were notified on 10 February 2026 and came into force on 20 February 2026. Their main features, as reported in commentary on the notification, are:

- a definition of synthetically generated information;
- an obligation on intermediaries to ensure that SGI carries a prominent label and permanent metadata or provenance identifiers;
- a clarification that references to "information" in provisions on unlawful acts include SGI, so deepfakes are treated like other unlawful content;
- duties on platforms to deploy reasonable technical measures to detect and prevent unlawful SGI; and
- compressed takedown timelines.

The amendment is significant because it moves from case-by-case injunctions to a systemic compliance regime. It also faces limits. Labelling informs viewers but does not undo reputational damage, labels and metadata can be removed or avoided by non-compliant tools, the definition excludes text, and enforcement against offshore services remains difficult. Exact timelines and wording should be quoted from the Gazette notification.

ISSN: 2582-6433

Judicial Response

Delhi High Court

The Delhi High Court has been the principal forum. Anil Kapoor v. Simply Life India (2023) was an early order restraining AI-based misuse of the actor's persona. In 2026, a steady series of interim orders followed. In Akira Nandan v. Sambhawaami Studios LLP, CS(COMM) 68/2026 (23 January 2026), the court granted an interim injunction against an AI-generated film and deepfake videos, treating personality, publicity and privacy rights as evolving doctrines that extend to AI avatars, synthetic voices and deepfake visuals. Similar protection was granted to Pawan Kalyan (January 2026), Kajol (February 2026), Ramdev (26 February 2026), Bhuvan Bam (May 2026), Yuvraj Singh in CS(COMM) 796/2026 (reported as 2026 LiveLaw (Del) 715), Tabu (August 2026) and Rajat Sharma (September 2026). The Bhuvan Bam matter is instructive because the plaintiff returned to court after infringement continued despite an earlier order, showing the limits of reactive injunctions.

Bombay High Court

In Arijit Singh v. Codible Ventures (2024) the Bombay High Court restrained AI voice cloning, and in Asha Bhosle v. Mayk Inc. (2025) it protected the singer against AI-generated voice and likeness. In the Preity Zinta matter (2026) the court ordered removal of AI deepfakes and reminded intermediaries such as Meta and Google to comply with the IT Rules.

Other decisions

Jackie Shroff v. The Peppy Store (Delhi HC, 2024) extended protection to a distinctive persona and expression. Public-interest litigations before the Delhi High Court, including those by Rajat Sharma and Chaitanya Rohilla, raised the regulation of deepfakes at a systemic level. Commentary also points to a 2025 Madras High Court decision titled X v. Union of India on digital safety, which should be read in full before it is relied upon.

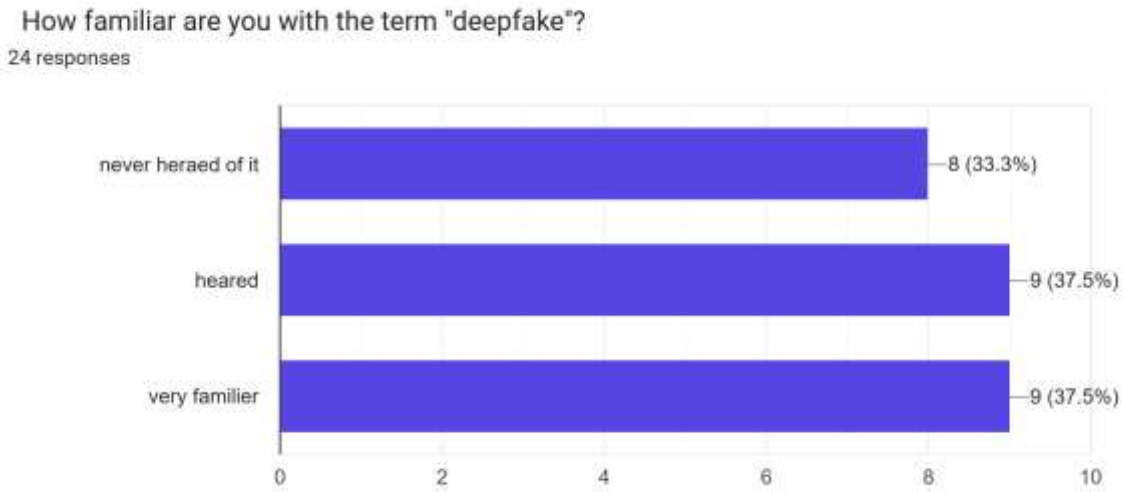
Analysis

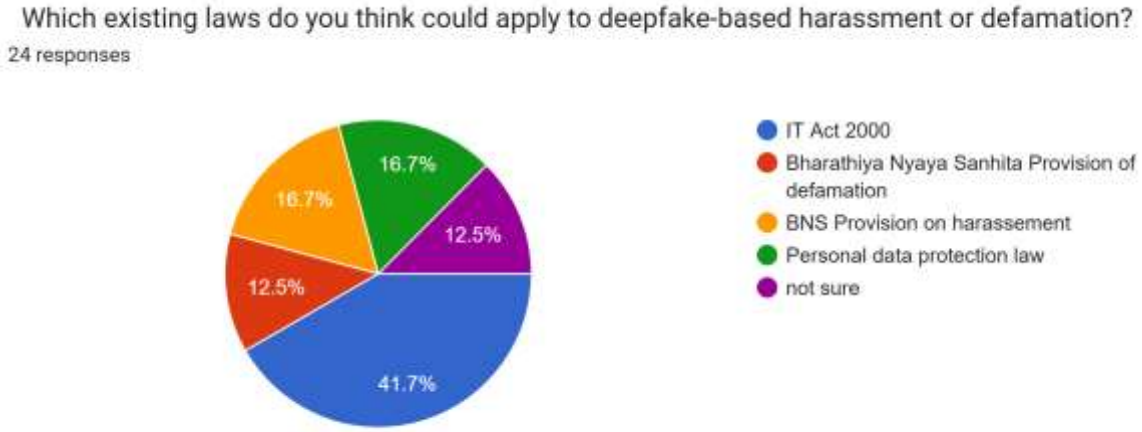
Four patterns emerge. First, courts reason from privacy, dignity and personality rights rather than the narrow law of defamation. Second, relief is typically ex parte interim injunctions against unnamed defendants (John Doe orders) with takedown directions to platforms. Third, beneficiaries are overwhelmingly public figures with commercial value. Fourth, there is little final adjudication, so doctrinal limits, such as the boundary between deepfakes and legitimate satire, remain untested.

ISSN: 2582-6433

Empirical Findings: Public Opinion Survey

The survey was conducted among [N] respondents between [date] and [date] through an online questionnaire. Respondent profile: [age range, gender split, education, location]. The results below are to be inserted from the actual responses; no figures are reported until data are collected

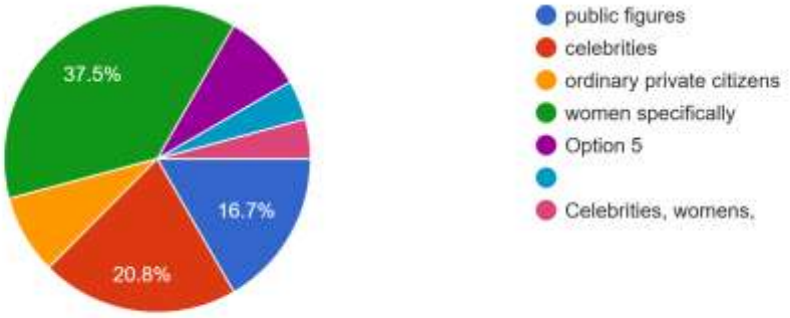




ISSN: 2582-6433

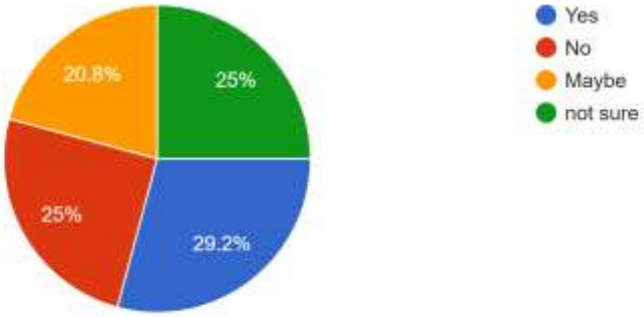
In your opinion, which of these is most at risk from deepfake misuse?

24 responses



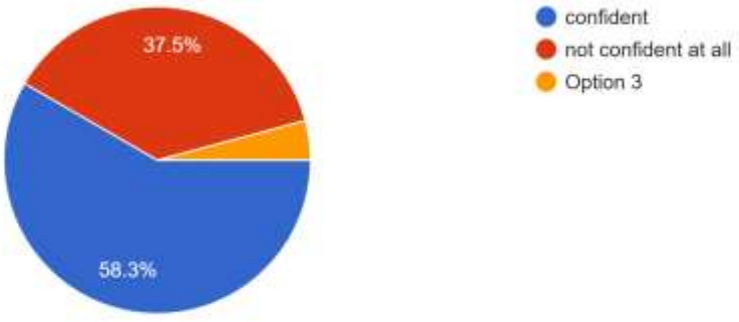
Are you aware of any Indian law that directly addresses deepfakes or synthetic media?

24 responses

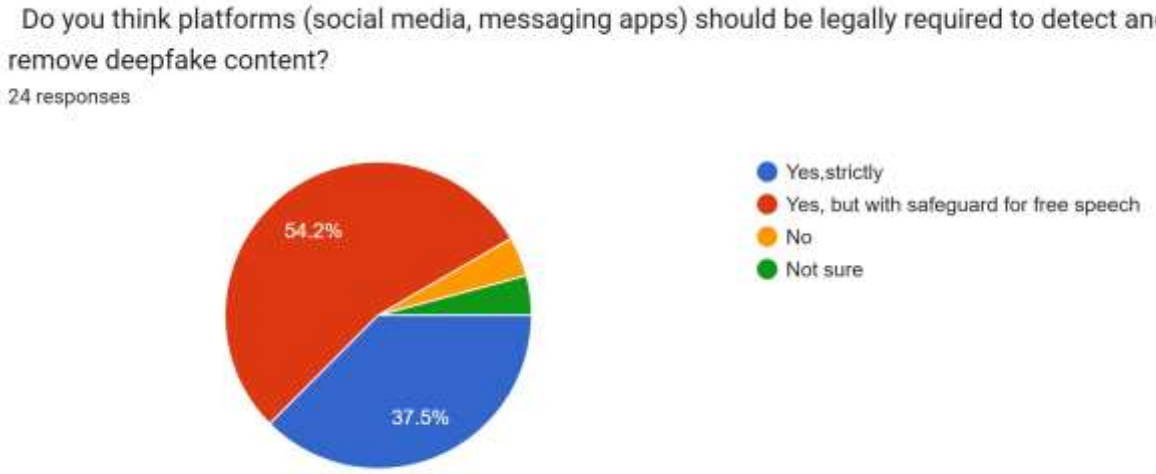


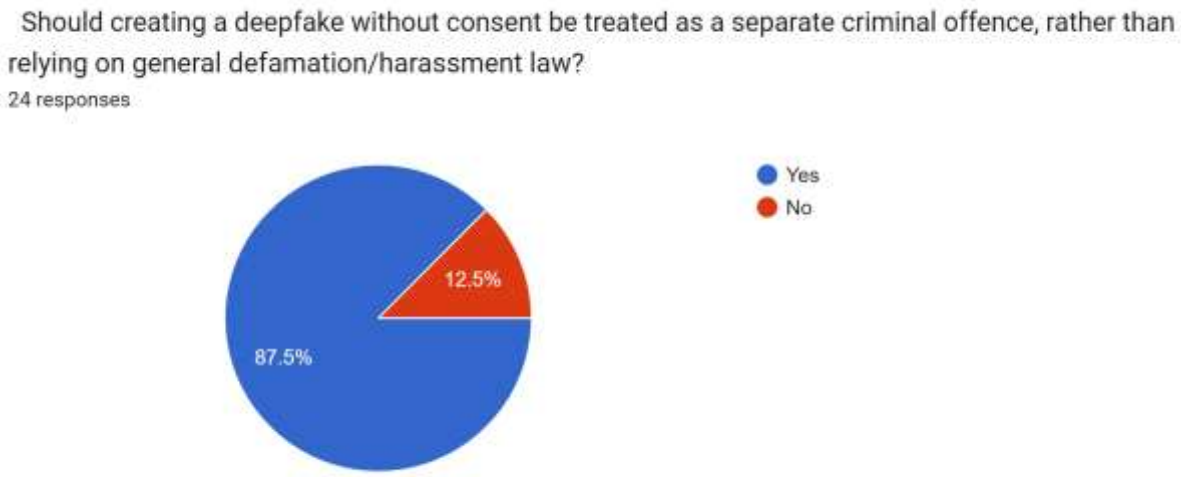
If someone is defamed or harassed using a deepfake, how confident are you that Indian law can provide an effective remedy?

24 responses



ISSN: 2582-6433





Comparative Perspectives

The European Union's Artificial Intelligence Act imposes transparency obligations on providers and deployers of systems that generate synthetic content. In the United States, federal legislation on non-consensual intimate imagery, including the TAKE IT DOWN Act, and a number of state laws on election and sexual deepfakes address specific harms. China's rules on deep synthesis require labelling and consent. Check the present status and text of each instrument before citing, as these laws are changing quickly. The common lesson is a mix of platform duties, labelling, and targeted offences for the most serious harms, rather than reliance on general defamation law.

ISSN: 2582-6433

Challenges

1. Attribution and anonymity of creators, and cross-border hosting.
2. Speed of spread against slow civil and criminal processes.
3. Reliance on personality rights, which favours the famous.
4. Fragmented provisions with no deepfake-specific offence or victim-centred civil remedy.
5. Balancing removal duties against freedom of expression, satire and parody, and avoiding over-removal by platforms.
6. Limits of detection and labelling technology, and the "liar's dividend".
7. Evidentiary difficulty in proving that media is synthetic.

Suggestions

1. Enact a specific offence for malicious, non-consensual deepfakes, with aggravated penalties for sexual content, election interference and fraud.
2. Codify personality and dignity rights by statute so that they extend beyond celebrities, with a fast-track civil remedy for private individuals.
3. Establish time-bound takedown and hash-matching or re-upload prevention duties for platforms, and a grievance appellate mechanism with transparency reporting.
4. Strengthen forensic capacity, including certified detection tools and clear rules on digital evidence.
5. Protect satire, parody, journalism and research through explicit exceptions with a clear public-interest test.
6. Provide victim support: dedicated cyber cells, legal aid and psychological support, and public awareness campaigns.
7. Pursue international cooperation on cross-border evidence and takedown.

Conclusion

India's response to deepfake-based defamation and harassment has been resourceful but incomplete. Courts have adapted personality rights to give swift relief to public figures, and the 2026 amendment to the IT Rules creates a first systemic regime for synthetic media. Yet the law remains scattered across statutes, reactive in operation and centred on those with commercial reputations. Ordinary victims still depend on slow criminal processes and general provisions never designed for synthetic media. A coherent, rights-based statute, supported by

ISSN: 2582-6433

proportionate platform duties and strong safeguards for free expression, is needed. [Add one sentence on whether the survey supported H1 and H2.]

References

Statutes and subordinate legislation

- Bharatiya Nyaya Sanhita, 2023.
- Information Technology Act, 2000.
- Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, as amended, including the Amendment Rules, 2026 (notified 10 February 2026, in force 20 February 2026).
- Copyright Act, 1957.
- Digital Personal Data Protection Act, 2023.
- Constitution of India, arts. 19 and 21.

Cases

- K.S. Puttaswamy v. Union of India (2017) 10 SCC 1.
- Shreya Singhal v. Union of India (2015) 5 SCC 1.
- Subramanian Swamy v. Union of India (2016) 7 SCC 221.
- DM Entertainment Pvt. Ltd. v. Baby Gift House (Del HC, 2010).
- Anil Kapoor v. Simply Life India (Del HC, 2023).
- Jackie Shroff v. The Peppy Store (Del HC, 2024).
- Arijit Singh v. Codible Ventures LLP (Bom HC, 2024).
- Asha Bhosle v. Mayk Inc. (Bom HC, 2025).
- Akira Nandan v. Sambhawaami Studios LLP, CS(COMM) 68/2026 (Del HC, 23 January 2026).
- Yuvraj Singh v. John Does, CS(COMM) 796/2026 (Del HC, 2026).
- Orders in the matters of Pawan Kalyan, Kajol, Ramdev, Bhuvan Bam, Tabu, Rajat Sharma (Del HC, 2026) and Preity Zinta (Bom HC, 2026): add full case titles, numbers and dates from the orders.

Secondary sources

- Robert Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753.

ISSN: 2582-6433

- Danielle Keats Citron, 'Sexual Privacy' (2019) 128 Yale Law Journal 1870.
- Add further books, journal articles, law commission or parliamentary committee reports, and law-firm or news commentary actually consulted, in OSCOLA or the format required by your department.

IJLRA