The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2026
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

DEEPFAKES AND THE LAW: A GROWING LEGAL CHALLENGE

Imagine a video of someone you know saying and doing things they never did. Their face, voice and movements look authentic, yet the video is AI-fabricated. This is a deepfake.

AI has brought remarkable benefits but also complex legal challenges involving privacy, consent and fraud. Deepfake technology, originally developed for lawful purposes such as entertainment, education, filmmaking, satire and accessibility, becomes a legal problem when used to deceive, defame, harass or hurt someone.

India's statutory framework is insufficient to address deepfakes, which threaten autonomy, privacy, freedom of expression, consent and reputation. There laws punishing deepfake creation but not for its regulation. Therefore, it creates needs to strengthen statutory framework to balance individual rights with legitimate uses of AI.

UNDERSTANDING DEEPFAKES

Deepfakes are AI-generated synthetic media (video, audio, etc.) intended to convincingly depict a person saying or doing something they never did. They can take several forms like voice cloning, synthetic video calls, and AI-generated content to mimic the way individuals communicate"[1]. The term 'deepfake' comes from fusion of words 'deep learning' and 'fake'. The creation of deepfakes involves three stages:

- Training: In this stage the AI system is fed with large amount of data related to targeted individual in order for system to learn about that individual. The larger the data the better the deepfake.
- Generation: In this stage, the system produces synthetic media replicating the patterns of the data studied by it in training stage.
- Real-time synthesis: This is the final stage wherein the synthetic media generated is produced on real time basis allowing the user to integrate it into a live phone call or video conference without having used any pre-recorded content.

It is for this reason that deepfakes can be developed using techniques of artificial intelligence and machine learning. Although deepfake systems were traditionally linked with the use of

[1] https://www.proofpoint.com/us/threat-reference/deepfake

The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2026
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

GANs, the development of generative AI technologies has brought about different ways of developing deepfakes.

Deepfakes can take multiple forms on the basis of the technologies and processes used to generate them. Face swapping replaces a target's face with another's in a video or image, reproducing expressions and movement. Lip-syncing and audio overlays alter video so that lip movement matches altered speech. Voice-only cloning replicates a target's voice to make it seem they are speaking. Full-body reenactment manipulates bodily movements and expressions to show actions never performed. Text-based conversational clones imitate a person's writing style by analysing their past communication.

The ability to reproduce a person's face, voice, expressions and manner of communication raises serious concerns about autonomy, privacy, reputation and consent, and enables impersonation, deception and other digital harm.

THE HARMS AND CHALLENGES

Originally developed to benefit society, deepfake technology is now widely misused to harm autonomy, privacy, reputation and consent through authentic-looking content that blurs reality and fabrication.

Malicious deepfakes mostly target celebrities, public figures and politicians to tarnish their image. A recent case involved actress Rashmika Mandanna, whose face was morphed onto an Instagram video posted by British-Indian woman Zara Patel.[2] It went viral, raising concern about AI-created deceptive, non-consensual content. This is just not limited to public figures but also ordinary individual faces its repercussion. Through deepfakes recipients are deceived by false claims presented as authentic, while the person impersonated suffers harm to autonomy, consent, privacy and reputation.

Sexually explicit deepfakes, created without consent or knowledge, are used to harass, exploit, humiliate or blackmail, including as revenge porn. Women are the primary targets, but men are not immune: morphed images and videos have been used to harass, threaten, extort or exploit them.

Deepfakes cause physical, financial, psychological and societal harms. Most malicious deepfakes online are pornographic and overwhelmingly target women, causing intense distress,

[2]https://www.bbc.com/news/world-asia-india-67305557

The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2026
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

trauma and reputational damage and enabling blackmail. In financial fraud, cybercriminals clone voices and videos to impersonate executives and relatives and trick victims into unauthorised transfers or disclosing information, using tactics such as OTP hacking, distressed-relative scams and hyperlink scams. In disinformation and political interference, fake videos and audio of politicians and candidates manipulate public opinion, injure reputations and destabilise democratic institutions. Fabricated media also erodes public trust: it hampers trust in journalism and digital records, and lets wrongdoers dismiss genuine evidence as a "deepfake".

Targeted individuals also face legal challenges. Article 21[3] protects privacy, held a fundamental and inalienable right in *Justice K.S. Puttaswamy v. Union of India* (2017).[4] A person's face, voice and likeness form part of their identity, and using them without consent violates privacy and autonomy. Section 356 of the BNS, 2023 protects reputation, and malicious deepfakes using fabricated content can qualify as defamation. Deepfakes is a major way of impersonation and identity theft, wherein, the creator creates deepfake of targeted and individual and can take their identity to deceive others. The information technology act provides for dealing with this under sections 66C and 66D.

STATUTORY FRAMEWORK

The following laws and rules aim to ensure an open, safe and accountable digital space.

THE INFORMATION TECHNOLOGY ACT, 2000 ("IT ACT")[5]

The IT Act does not specifically regulate deepfakes, but some provisions apply. Section 43 prescribes penalty and compensation for unauthorised acts involving computer systems and data,[6] and section 66 covers computer-related offences.[7] The Act also addresses identity theft (66C), impersonation (66D), privacy violations (66E)[8] and publishing obscene or sexually explicit content (67, 67A).[9] Deepfakes amounting to these offences can be tackled, though the

[3]Constitution of India 1950, art 21
[4]Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1
[5]The Information Technology Act 2000
[6]The Information Technology Act 2000, s 43
[7]The Information Technology Act 2000, s 66
[8]The Information Technology Act 2000, ss 66C, 66D, 66E
[9]The Information Technology Act 2000, ss 67, 67A

The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2026
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

Act does not address deepfakes independently, which requires victim to prove that deepfake fits into the scope of the framework.

THE BHARATIYA NYAYA SANHITA, 2023 ("BNS")[10]

The BNS supplements the IT Act. Section 319 punishes cheating by personation,[11] section 336 punishes forgery, including false electronic records made to cheat or harm reputation,[12] and section 353 penalises false or misleading statements, rumours or reports causing public mischief or fear.[13] Organised cybercrime involving deepfakes falls under section 111.[14] The BNS punishes the consequences of deepfakes but does not make deepfakes a crime independently.

THE INFORMATION TECHNOLOGY (INTERMEDIARY GUIDELINES AND DIGITAL MEDIA ETHICS CODE) RULES, 2021 ("IT RULES")[15]

Intermediaries must exercise due diligence and inform users not to host, share or transmit information that belongs to another person; is obscene, pornographic, invasive of privacy, or promotes hate or violence; deceives about the origin of a message; knowingly communicates misinformation or patently false information; impersonates others, including via AI; threatens national security or public order; or violates any law. These rules are of importance because deepfakes spreads rapidly through online platforms, thereby amplifying harm before an affected individual can obtain an effective remedy. These rules can regulate deepfake as these rules mostly revolves around components of deepfakes

GRIEVANCE REDRESSAL MECHANISM

Intermediaries must appoint Grievance Officers and conduct hearings on complaints. Users are allowed to lodge appeals on grievances if they have not been addressed, ensuring accountability and transparency. Through this mechanism aggrieved person whose identity was fabricated through deepfakes can reach out to these intermediaries and thereby address their grievances.

RECENT AMENDMENTS

'The IT Rules 2021 were amended to include changes to address synthetic generated information (SGI) including deepfakes and other AI generated content on 10 February 2026.

[10]The Bharatiya Nyaya Sanhita 2023
[11]The Bharatiya Nyaya Sanhita 2023, s 319
[12]The Bharatiya Nyaya Sanhita 2023, s 336
[13]The Bharatiya Nyaya Sanhita 2023, s 353
[14]The Bharatiya Nyaya Sanhita 2023, s 111
[15]The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021

The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2026
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

There is a requirement that intermediary needs to label and add traceable metadata to lawful AI generated content. The new regulation provides for strengthened due diligence and user's responsibility, including an obligation on users to be aware of legal consequence of actions. Explicitly included is a definition of child sexual exploitation material, nonconsensual intimate imagery, impersonation and harmful content using AI.

The time period for removals based on actual knowledge (government notification or court order) have been reduced from 36 to 3 hours. The grievance redressal time period has been reduced from 72 to 36 hours and 24 to 2 hours where the matter involves nudity or impersonation. There is a requirement on intermediaries to take reasonable technical measures, including automation where possible, to stop SGI if the content violates any law. The Significant Social Media Intermediaries are also required to take reasonable efforts to automatically detect and remove content depicting rape or child sexual abuse, or content identical to previously removed content.'[16]

THE WAY FORWARD

Malicious deepfakes can be reduced through these measures. *Firstly*, strict penalties for malicious deepfakes involving fraud, impersonation, identity theft and especially non-consensual sexual imagery would deter offenders. *Secondly*, safeguards should be quick, simple and cheap, with transparent proceedings, proper notice, a fast internal appeal and a reasonable hearing. *Thirdly*, personality and likeness rights need a stronger statutory footing so ordinary individuals, not only celebrities, can seek protection and compensation. *Fourthly*, digital evidence should be examined carefully and thoroughly for verifying its authenticity. *Finally*, public awareness should be raised through literacy campaigns and simple verification habits.

[16] https://www.pib.gov.in/PressReleasePage.aspx?PRID=2295500&reg=48&lang=2

The Indian Journal for Research in Law and Management
Open Access Law Journal – Copyright © 2026
Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

CONCLUSION

The abuse of deepfakes is currently a major legal and societal issue since it endangers individual's rights like autonomy, privacy, consent, and reputation and can cause acts such as impersonation, fraud, harassment, and disinformation against individuals.

In India, the statutory framework involves laws such as the IT Act of 2000; BNS, 2023; IT Rules, 2021; and SGI amendments. However, problems still exist with respect to identifying wrongdoers, collecting electronic evidence, and providing remedies since there might be an insufficient number of legislations to solve all problems.

The ideal framework should protect rights without preventing artificial intelligence from being used for educational, cinematographic, satirical, and accessibility purposes. This can be achieved by improving enforcement, grievances redressal, detecting technology, platform responsibility, and awareness campaigns. The goal is not to stop technological progress but promote it in a way that maintains human dignity.