INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed

www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

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IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines.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 All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice.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 DEEP FAKE TECHNOLOGY IN INDIA: LEGAL CHALLENGES IN PROTECTING WOMEN ONLINE.

AUTHORED BY - MADHUMITA CHAUDHARY

The rapid development of artificial intelligence and digital technologies has transformed the way information is created and shared, while also introducing new challenges. Deepfake technology, in particular, raises serious concerns as it can be misused to spread misinformation, harm reputations, and violate privacy.

INTRODUCTION

In the digital age, communication among people has changed significantly because of modern technology. However, developments in technology have also led to an increase in cybercrime. Deepfake, as an advanced technology, can also be used for harmful and illegal activities.

According to data from the National Crime Records Bureau (NCRB), cybercrime in India increased by 24.4% in 2022, with 65,893 cases reported. The misuse of deepfake technology, especially against women, has become an important issue.

This problem is growing because the number of internet users in India is increasing rapidly, with more than 900 million people now using the internet. As more people go online, the risk of cybercrime and the misuse of technologies like deepfakes may also increase.

Deepfake technology uses artificial intelligence (AI) to create fake but very realistic videos, audio, or images. These can make it appear as if a person said or did something that never actually happened. In India, some laws try to deal with online crimes and privacy violations. For example, the Information Technology Act, 2000 includes certain sections that address these issues, such as Section 66E, which deals with the violation of a person's privacy, and Section 67, which deals with publishing vulgar content online.

However, these laws do not mention deepfake technology specifically, and there is no clear

ISSN: 2582-6433

rule that directly regulates deepfakes. This is especially concerning for women, who are often targeted through fake videos or images online. Therefore, stronger and clearer regulations are needed to prevent digital exploitation.

The research in this study uses a doctrinal research method. This means the study is based mainly on existing documents and written sources rather than surveys or experiments. The researcher examines secondary sources such as academic articles, legal commentaries, reports, and online materials.

The study also analyses important laws, including the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023, to understand how current legal rules deal with cybercrime and digital privacy.

UNDERSTANDING DEEPFAKE TECHNOLOGY

Deepfake is a technology in which images, videos, or audio are manipulated or replaced with fake content so that it appears as if a person said or did something that never actually happened. This technology is created using artificial intelligence. A type of AI known as Generative Adversarial Network (GAN) is commonly used to produce fake videos, photos, and audio.

In this system, two models work together. The first model generates fake content (generator), while the second model evaluates whether the content appears real or fake (discriminator). By repeating this process many times, the generated media becomes highly realistic and difficult to detect.

However, this technology can have negative effects because it may spread misinformation and reduce people's trust in digital media. Despite these risks, deepfakes can also be used for positive purposes such as entertainment, filmmaking, and creative content production.

DeepFaceLab and Faceswap are two software tools that are used to create fake videos and voices. These tools work by first collecting videos and images of a person and then analysing their facial structure. In the second step, the system learns how the person's face moves using artificial intelligence. After learning these movements, the tool swaps the face of one person with another person's face in a video or image. This process is carried out smoothly, making

ISSN: 2582-6433

the final result appear realistic and difficult to detect as manipulated content.

Once these fake videos or images are created, they can spread very quickly on social media platforms such as YouTube, Twitter, and Facebook. Fake or anonymous accounts often share this content repeatedly, which can spread false information and make it difficult to identify the original source.

Deepfakes are often used in negative and harmful ways. For example, someone can create fake videos by placing a person's face onto another person's body without their permission. This technique is frequently used to produce pornographic content, and women often become the primary victims in such cases. People may also use deepfakes to harass individuals or damage their reputation.

Criminals can exploit this technology to impersonate someone else, such as a company executive, in order to commit fraud. Deepfakes can also be used to spread misinformation by creating fabricated videos that show individuals giving speeches or performing actions that never actually occurred.

Due to such misuse, deepfakes can cause serious emotional and psychological harm to victims. Furthermore, they can reduce public trust in digital media, as it becomes increasingly difficult for people to distinguish between real and manipulated content online.

Deepfakes can seriously harm women's dignity and reputation. This technology can be misused by placing a woman's face into pornographic videos without her consent. Such actions represent a clear violation of an individual's privacy. As a result, victims often suffer damage to their reputation, emotional distress, and, in some cases, social isolation.

Many cases involve the creation of fake content using the faces of female celebrities and professionals. Due to the misuse of deepfake technology, women may feel unsafe or discouraged from participating in public discussions, social media, or professional activities. This misuse also contributes to increased online harassment and gender-based violence.

ISSN: 2582-6433

Legal Framework

1. Information Technology Act, 2000

India has several laws to deal with online activities, with the Information Technology Act, 2000 being the most important. It provides rules to regulate digital platforms, prevent cybercrime, and protect users from online threats. However, with new technologies like deepfakes, new risks have emerged. Deepfakes can create highly realistic fake videos, images, or audio, which can be misused for identity theft, spreading misinformation, or creating explicit content without consent. While existing provisions such as Sections 66E, 66D, and 67 deal with privacy violations, impersonation, and obscene content, they do not explicitly address deepfake technology. As deepfakes become more advanced and widespread, it is important to update existing laws to effectively regulate their misuse and ensure better protection for individuals in the digital space.

2. Bharatiya Nyaya Sanhita

The Bharatiya Nyaya Sanhita, 2023 has replaced, the Indian Penal Code, 1860 as the main criminal law in India. This new law deals with many types of crimes, including some offences that can occur online. Just like the IT Act, this law does not contain specific provisions that directly address deepfake technology. Instead, some general legal provisions may be used to deal with problems caused by deepfakes.

Some sections of the Bharatiya Nyaya Sanhita can be applied in cases of deepfake misuse. To start with, Section 294 punishes people who perform or share obscene acts or words in public. If someone creates or spreads explicit deepfake content, this section could apply.

Moving further, Section 356 deals with harm to a person's reputation through words, signs, or other forms of communication. We also have Section 316, which applies when someone deceives another person to cause financial or personal loss. Deepfakes used for impersonation or fraud, such as pretending to be another person, may fall under this provision.

Although these sections can be used in cases involving deepfakes, they are general laws and were not designed specifically to address artificial intelligence technologies. Because of this, there may be gaps in enforcement, making it difficult to effectively regulate deepfake-related crimes.

3. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021

Platforms such as Facebook, X, and YouTube are treated as online content hosts because they

ISSN: 2582-6433

enable the hosting and sharing of user-generated content. In this role, they act as gatekeepers, responsible for supervising and managing online content, including deepfake videos. There are certain responsibilities of social media platforms, and to start with:

"Platform Obligations," wherein social media companies must clearly state in their policies that users are not allowed to post illegal or harmful content, such as deepfake videos, misinformation, or vulgar material. They must also keep user information and records so that authorities can investigate cybercrime when needed.

The other is the **"Duty to Remove Harmful Content."** In this, when harmful content such as deepfake videos is reported, the platform must remove it within 36 hours of receiving the complaint. Significant Social Media Intermediaries (SSMIs) are also required to appoint Grievance Officers to handle such complaints.

4. Grievance Redressal System

Platforms are required to establish a round-the-clock complaint mechanism through which users can report harmful content. They must acknowledge and address such complaints within a period of 15 days. In cases where the issue remains unresolved, it may be escalated to higher government authorities for further consideration and action.

5. Right to Privacy (Basic Idea)

When it comes to the right to privacy, one of the important cases we talk about is Justice K.S. Puttaswamy (Retd.) v. Union of India.

After the Puttaswamy judgment, courts have also started recognizing personality rights, which means a person has control over how their name, image, and identity are used. So, if someone creates a deepfake without permission, it can be treated as a violation of privacy rights, and the victim can take legal action (civil or criminal).

The privacy of an individual is a fundamental right, as stated by the Supreme Court. This right comes under:

Article 21 – Right to life and personal liberty: It states that every person has the right to live freely and safely. No one can take away this right except according to the procedure established by law.

Article 14 – Right to equality: It ensures that everyone is equal in the eyes of the law, and the government must treat all people fairly without discrimination.

Article 19 – Right to freedom: It guarantees certain freedoms, such as freedom of speech and expression.

ISSN: 2582-6433

All these rights clearly state that every person has the right to control their personal life, personal information, and to live with dignity.

Deepfake technology can seriously violate these rights in many ways. For example, if someone creates a fake video containing vulgar content by replacing a person's face with another person's face, it can harm the self-respect of the individual, which relates to Article 21. Deepfakes can also be used by adding a person's face to videos or images without permission. This means the person loses control over their identity and personal data, which is a violation of privacy.

Deepfakes can also be used to impersonate someone, which can harm their reputation or be used for fraud and misinformation. This directly affects a person's identity and personal image.

Legal Challenges and Gaps in India

India's legal framework for dealing with deepfakes is still developing and is not strong enough to address the issue effectively. There are several gaps in the current system, particularly when it comes to protecting individuals online, with women being especially vulnerable to such misuse.

1. No Specific Law for Deepfakes

India does not have a specific law to regulate deepfake technology. Existing laws such as the Information Technology Act, 2000, and the Bharatiya Nyaya Sanhita, 2023 address issues like cheating, impersonation, privacy violations, obscenity, and defamation. However, these laws were not designed for AI-based content and are not fully effective in dealing with deepfake-related offences.

2. Misuse Against Women

Deepfakes are often used to create non-consensual and harmful content targeting women. Current laws do not clearly address misuse of a person's face or voice, which are important aspects of identity. Cases like that of Rashmika Mandanna highlight how victims may suffer reputational harm and emotional distress without adequate legal protection.

3. Difficulty in Identifying Criminals

Identifying offenders is difficult because they can hide their identity using tools like VPNs and operate through foreign servers. Deepfake content also spreads rapidly across borders, making investigation and legal enforcement more complex.

ISSN: 2582-6433

4. Weak Accountability of Social Media Platforms

The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 require platforms to remove harmful content within 36 hours. However, enforcement is often inconsistent, allowing such content to spread before it is removed.

5. Need for Stronger Laws

There is a need for clearer and stronger laws, improved identification methods, greater platform responsibility, and international cooperation to effectively regulate deepfake-related crimes.

RECOMMENDATION AND LEGAL REFORMS

1. Need for Legal Reforms

India needs stronger and clearer laws to deal with deepfake technology. The current laws are not enough, so new rules and changes are needed to better prevent its misuse.

2. Specific Law for Deepfakes

There should be a separate law or amendments to the Information Technology Act, 2000 that clearly define deepfakes. The law should describe deepfakes as AI-generated content created without a person's consent and provide strict punishments, which should include imprisonment and heavy fines, especially in cases involving harmful content. This would help address the gaps present in existing laws such as the Bharatiya Nyaya Sanhita, 2023.

3. Better Investigation System

There is a need for improving the way in which cybercrimes are investigated. This can be done by setting up cyber police units and training them in AI and digital forensics, and using technologies like deep fake detection and data tracking. This will help in catching the criminals more efficiently, even if they are from different countries.

4. Responsibility of Social Media Platforms

Social media platforms should have stronger responsibilities under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021. They should monitor the content in real time, use tools such as watermarking to detect AI-generated content, remove harmful content quickly, and provide reports explaining how such issues are handled.

These measures aim to maintain a balance between innovation and safety, while stressing the

ISSN: 2582-6433

importance of taking legislative action by 2027.

CONCLUSION

Deepfake technology is becoming a serious issue, especially for women, as it can harm their dignity, privacy, and participation in online spaces. In India, laws like the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 deal with cybercrime, but they are general and do not specifically address deepfakes.

Although the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India recognized privacy as a fundamental right, there are still no strong systems to prevent the misuse of personal images and videos through deepfakes.

Because of these gaps, offenders can hide their identity, harmful content spreads quickly, and women are often targeted. The case of Rashmika Mandanna shows how serious the impact can be. Studies also suggest that a large amount of deepfake content online is non-consensual and mainly targets women.

To deal with this problem, India needs clear laws on deepfakes, stricter punishments, better investigation methods, and faster removal of harmful content by social media platforms. Awareness programs and simple complaint systems can also help victims.

Without timely action, deepfakes may reduce trust in digital platforms and discourage women from participating online.

REFERENCE

- Jain, R. (2025, October 6). *NCRB data on cyber crimes dated, not indicative of true picture: Experts*. BOOM. https://www.boomlive.in/news/ncrb-report-notes-sharp-rise-in-cyber-crimes-in-india-29662
- Arya, K. (2025, December 16). *Deepfake regulation India 2025: MeitY's comprehensive IT rules amendment*. Khurana & Khurana. https://www.khuranaandkhurana.com/deepfake-regulation-india-2025-meity-s-comprehensive-it-rules-amendment

ISSN: 2582-6433

- Government Technology Agency of Singapore. (n.d.). *What are deepfakes?* Digital for Life. https://www.digitalforlife.gov.sg/learn/resources/all-resources/what-are-deepfakes
- UT Southwestern Medical Center. (2024, November 22). *Deepfake*. https://www.utsouthwestern.edu/employees/information-security/awareness/updates/deepfake.html
- RFA Staff. (2023, February 8). *China's deepfake anchors spread disinformation on social media, Graphika says*. Radio Free Asia. https://www.rfa.org/english/news/china/china-deepfake-02082023032941.html
- Joe Morelle. (2025, March 6). *Congressman Joe Morelle announces renewed effort to combat harmful deepfake pornography*. https://morelle.house.gov/media/press-releases/congressman-joe-morelle-announces-renewed-effort-combat-harmful-deepfake
- Press Information Bureau, Government of India. (2026, February 11). *Under Mission Shakti, holistic and victim-centric approach is adopted to strengthen safety, security and empowerment of women, including protection against technology-facilitated crimes*. https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=2226335&reg=3&lang=2
- Chin, K. (2026, January 5). *Top cybersecurity regulations in India in 2026*. UpGuard. https://www.upguard.com/blog/cybersecurity-regulations-india
- Bajaj Finserv. (n.d.). *Cyber law in India*. https://www.bajajfinserv.in/cyber-law-in-india
- PRS Legislative Research. (2023). *The Bharatiya Nyaya Sanhita, 2023*. https://prsindia.org/billtrack/the-bharatiya-nyaya-sanhita-2023
- Ministry of Home Affairs, Government of India. (2023). *The Bharatiya Nyaya Sanhita, 2023*. https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf
- Government of India. (2021). *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021*. https://www.india.gov.in/category/science-it-communication/subcategory/digital-media/details/the-information-technology-intermediary-guidelines-and-digital-media-ethics-code-rules-2021
- IANS. (2024, February 20). *Social media platforms have legal obligation to curb deepfakes: MoS IT*. ET Government.

ISSN: 2582-6433

https://government.economictimes.indiatimes.com/news/governance/social-media-platforms-have-legal-obligation-to-curb-deepfakes-mos-it/107842803

- Reddy, P. (2017, August 26). *The Supreme Court's privacy judgment elevates personality rights to the constitutional plane*. SpicyIP. https://spicyip.com/2017/08/the-supreme-courts-privacy-judgment-elevates-personality-rights-to-the-constitutional-plane.html
- Supreme Court Observer. (n.d.). *Justice K.S. Puttaswamy v. Union of India: Fundamental right to privacy*. https://www.scobserver.in/cases/puttaswamy-v-union-of-india-fundamental-right-to-privacy-case-background/
- Chandel, J., & Kundu, M. (2025). *AI-generated deepfakes and the legal vacuum in India: A constitutional analysis of privacy, consent, and digital harm under Article 21*. *International Journal for Research Trends and Innovation*, 10(11). https://www.ijrti.org/papers/IJRTI2511099.pdf
- Mehta, K. (2025, October 6). *The persona paradox: Deepfakes & personality rights in India*. K&S Partners (Khurana & Khurana / KS&K). https://ksandk.com/media-and-entertainment/the-persona-paradox-deepfakes-personality-rights-in-india/
- Trivedi, G. (2025, November 18). *Deepfakes, identity, persona and the Indian legal frontier*. Chadha & Co. (C&CIP). https://www.candcip.com/single-post/deepfakes-identity-persona-and-the-indian-legal-frontier
- Mali, P. (2026, February). *AI laws and regulations in India as of 2026: A comprehensive overview for practitioners, businesses, and policymakers*. https://www.prashantmali.com/cyber-law-blog-india/ai-laws-and-regulations-in-india-as-of-2026
- Pandey, A. (2025). *Cyber law in India: Loopholes, legislative backwardness and the need for comprehensive reform*. *LawFoyer International Journal of Doctrinal Legal Research*, 3(4). https://lijdlr.com/2026/01/04/cyber-law-in-india-loopholes-legislative-backwardness-and-the-need-for-comprehensive-reform/
- California State Assembly Committee on Privacy and Consumer Protection. (2025). *SB 11 (Ashby): APCP analysis*. https://apcp.assembly.ca.gov/system/files/2025-07/sb-11-ashby-apcpanalysis.pdf
- Patel, R. (2025, November 7). *Me, myself and AI: Chasing deepfakes across borders without losing your rights*. SCC Online. https://www.scconline.com/blog/post/2025/11/08/deepfake-regulation-rights/

ISSN: 2582-6433

- India Today. (2023, November 10). *Rashmika Mandanna deepfake video: Delhi Police registers case*. https://www.indiatoday.in/india/story/rashmika-mandanna-deepfake-video-delhi-police-case-registered-2461547-2023-11-10
- Loux, M. (2025, September 11). *What is deepfake technology? Understanding its broad impact*. American Military University. https://www.amu.apus.edu/area-of-study/information-technology/resources/what-is-deepfake-technology/
- Acharya, M. (n.d.). *IT Act 2000: Objectives, features, amendments, sections, offences and penalties*. ClearTax. https://cleartax.in/s/it-act-2000