
MISUSE OF AI: DEEPPAKE IMAGES AND WOMEN: A NEW FORM OF CYBER VICTIMIZATION

Supriya Rani, Amity Law School

ABSTRACT

With the rise of AI, a growing array of new risks is emerging that disproportionately impacts women, one such being the misuse of deepfakes. Digital content can be manipulated even with sophisticated AI methods, such as machine-learning models such as Generative Adversarial Networks (GANs), to superimpose an individual's likeness onto fabricated images and videos, even if they are of a sexually explicit or misleading nature, without their awareness or consent. These practices have led to the development of new ways of cyber victimisation that pose important legal and ethical issues. In this paper, the author looks at the doctrinal aspects of the harms caused by deepfakes and assesses how the current Indian legal regime is able to meet such threats. It examines the provisions of the Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023, Digital Personal Data Protection Act, 2023, and constitutional protections, as provided in Indian law. The study also places the Indian legal response in the wider international context by looking at the international legislative and regulatory developments in the European Union and the United States. The paper also examines some of major concerns surrounding the evidence standards, the duty of intermediate platforms and the constitutionality of privacy, dignity and personal autonomy. It recommends a suite of doctrinal and legislative proposals to bolster the legal response to cyber victimisation using deepfakes and improve the protection of victims.

Keywords: Deepfakes, Cyber Victimization, Artificial Intelligence, Women's Rights, Information Technology Law.

1. Introduction

One of the most serious legal issues at present is the interconnection between artificial intelligence and gender-based violence. The word “deepfake” has been coined out of the words “deep learning” and “fake.” Deepfake refers to the digital manipulation of content using sophisticated machine learning techniques. The technology is capable of producing fabricated audio or visual content that seems to depict a person performing some actions or speaking in a manner not done before.¹

Despite the positive implications of the use of deepfakes in various industries, including the medical field, educational institutions, and the entertainment industry, the unethical application of deepfakes through the creation of non-consensual pornographic images of women is considered an infringement of privacy and human dignity. According to the research carried out in 2019 by Deeptech, a cybersecurity firm, 96% of deepfake videos found on the internet had pornographic content, with the victims being mostly women.²

Due to its large population that uses the internet and an emerging system of artificial intelligence, India has been exposed to various risks owing to the use of deepfake technology. The use of deepfake technology by hackers to target actresses, journalists, and other celebrities has led to widespread attention being drawn towards the matter. However, despite all these events, the laws governing the use of deepfake technology have been very weak and fragmented. The Information Technology Act of 2000, which is the main law for cyber activities in India, does not cover deepfakes.³

2. Deepfake Technology and the Victimization of Women

a. Technical Architecture of Deepfakes

To adequately gauge the legal challenges of deepfakes, it is necessary to grasp how deepfakes are created. The Generative Adversarial Network (GAN) is one of the key technologies in the creation of deepfakes, an AI framework that was introduced in 2014 by Ian Goodfellow and

¹ Shalvi Suchi, Arvind Kumar, Anjum Parvez, Radhey Shyam Jha & Deependra Nath Pathak, “Protection of Children from the Evil of Pornography”, 6(S1) *International Journal of Health Sciences* 14001, 14001–14011 (2022).

² Information Technology Act, 2000 (Act 21 of 2000), s 66E; Information Technology (Amendment) Act, 2008 (Act 10 of 2009), s 66A (struck down by Supreme Court in *Shreya Singhal v Union of India*, AIR 2015 SC 1523).

³ Ian Goodfellow et al., 'Generative Adversarial Networks' (2014) 27 *Advances in Neural Information Processing Systems* 2672; see also Hao Li et al., 'Protecting World Leaders Against Deep Fakes' (CVPR Workshops, 2019).

his colleagues. A GAN works by having two neural networks: a generation that creates fake content and an evaluation that decides whether or not the generated output is authentic content. The generating network is trained repeatedly on large collections of real images and videos, and will increasingly improve its results, so the outputs become increasingly realistic, indistinguishable from real media. This can be used to create a “face-to-face” image of a person's face on another person's body, with surprising accuracy, even when applied to a very small set of social media–available images.

In addition to GANs, more sophisticated approaches such as diffusion models and neural radiance fields have boosted synthetic media in terms of its visual fidelity, emotional convincingly, and even consistency between video frames. The growth of open-source software, public code repositories and easy-to-use applications has greatly increased access to these technologies. This means that people do not need to possess any special technical expertise to make a convincing deepfake. Many commercial products and online services now allow people to create manipulated AV content with ease and at scale, allowing for greater potential for misuse and harm to innocent viewers.⁴

b. The Gendered Dimension of Deepfake Harm

The damage done to women by deepfakes is multi-faceted and very interconnected. Apart from the primary form of injury, this kind of media can cause damage to one's psychological state and lead to diseases such as anxiety, depression, PTSD, and, in some extreme cases, suicide. The ramifications can also include damage to a woman's reputation and result in her social isolation, problems at work, and family troubles. Another factor that makes this issue persistent is the speed and scale of the spread of materials on the Internet. Even if the fake video is identified and taken down from one platform, its copies may stay in circulation forever.⁵

From a wider perspective, the use of deep fakes against women is meant to reinforce the existing patriarchal regimes that aim at regulating and controlling women's bodies and sexuality.⁶ According to Professor Danielle Keats Citron, the production and dissemination of

⁴ Deeptrace Labs, 'The State of Deepfakes 2019' (September 2019) 7 available at: <https://deeptrace.com/report> (last visited on: May 14, 2026); see also Samantha Cole, 'AI-Assisted Fake Porn Is Here and We Are Not Ready' (Motherboard, December 2017).

⁵ National Commission for Women, Annual Report 2022-23 (NCW, New Delhi, 2023) <<https://ncw.nic.in>> accessed 12 March 2025.

⁶ Pallavi Singh & Radha Ranjan, “Sexual Harassment of Women at Work Place: A Study of Indian Legislation and Judicial Approach”, 4(1) *Indian Journal of Law and Legal Research* 1, 1–8 (2022).

consensual pornography violate the right of the victim to sexual privacy since the woman is used as an object for public viewing and consumption, which is often done by men.⁷ The threat of exposing the pictures is a type of gender-specific coercion. In general, the harm caused to individuals translates into the harm to society because it constrains the participation of women in digital space and in public.⁸

The reports that have been submitted yearly to the NCW reveal that cyberbullying and image-based abuse have continued to affect a significant number of people. There have been thousands of such cases reported in a year, revealing that the offenses are persistent in the online world. As well, the Crime in India 2022 report by the National Crime Records Bureau highlights many cases of cyberstalking, voyeurism, and electronic dissemination of obscene material. Nonetheless, it is challenging to measure the prevalence of deepfake offenses since there is no category under crime classification to distinguish such offenses. Moreover, many other cases are unreported owing to stigma and potential embarrassment.⁹

c. Taxonomy of Deepfake-Based Offences Against Women

To facilitate the process of legal scrutiny, it is beneficial to distinguish among the different types of offenses that can be committed using deepfake technology. The first type comprises offenses that arise from the production of fake sexual content, whereby someone is digitally depicted within pornographic content without his consent. The second kind comprises cases of reputational damage, whereby someone's reputation is damaged because of false depictions of the individual doing wrong or acting illegally, such as accepting bribes or being involved in crimes. The third type comprises cases of stalking or intimidation using deepfake content as tools of harassment or coercion.¹⁰

The fourth area that has gained legal recognition is the employment of deepfake technology in exploiting and grooming children through manipulation. The use of deepfake in these contexts generates its own legal issues related to child welfare. These four areas involve their own set

⁷ Radha Ranjan, "Evolution of the Doctrine of Proportionality: Assessing its Scope and Ambit in Relation to the Right to Privacy in India", 10(1) *Indian Journal of Law and Human Behavior* 31, 31–38 (2024).

⁸ Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press 2014) 247; see also Citron, 'Sexual Privacy' (2019) 128 *Yale Law Journal* 1870.

⁹ National Crime Records Bureau, *Crime in India 2022* (Ministry of Home Affairs, New Delhi, 2023) Table 5A.1 available at: <https://ncrb.gov.in> (last visited on: May 20, 2026).

¹⁰ Mary Anne Franks, 'Drafting an Effective Revenge Porn Law: A Guide for Legislators' (Cyber Civil Rights Initiative, 2015) available at: <https://cybercivilrights.org> (last visited on: May 22, 2026).

of legal rights and interests which include privacy, dignity, reputation, autonomy, and freedom from coercion.¹¹

3. The Indian Legal Framework

a. The Information Technology Act, 2000

The IT Act, 2000 is regarded as the main act of law relating to electronic commerce and cybercrimes in India.¹² The connection between the Act and the victims of deepfakes is not through the provisions of the act but from the interpretation of the law. One example of the section where the act is connected to the issue of victims of deepfakes is that of Section 67 where there is prohibition of publishing and transmitting of obscene material in electronic form. Section 67A of the act prohibits the dissemination and transmission of sexually explicit acts in electronic form.¹³

There are several major flaws related to the extent and interpretation of these regulations. Firstly, Clause 67 still uses the old concept of obscenity based on English common law and the Hicklin test according to which any material is evaluated depending on whether it might corrupt or affect the morals of people likely to see it. In terms of modern digital content, such approach seems outdated and controversial. Secondly, Clause 66E is mainly focused on the capturing or distribution of photos of a person's private parts without prior consent. Nevertheless, deepfake can create completely fake images which will not contain any real private photos of a victim. Thus, the regulation of Information Technology Act does not cover the creation, circulation, or storage of fake pornographic content.

Under the Information Technology Act, especially under Section 79 and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, there are some due diligence responsibilities for online platforms. It is expected from intermediaries to remove any illegal contents as soon as possible after receiving court orders and directions from the Government. The 2021 Rules also stipulate that it is mandatory for the Significant Social

¹¹ Radha Ranjan & Anupam Sinha, "Child Pornography Laws in India: A Comparative Legal Analysis with Global Frameworks", 11(3) *The Research Journal (TRJ)* 86, 86–99 (May–June 2025).

¹² Radha Ranjan, Bheem Singh Meena & Shyam Kumar Anand, "Virtual Meetings Under Attack: Assessing the Legal and Security Risks of Zoom Bombing in the Digital Era", 4(2) *ShodhKosh: Journal of Visual and Performing Arts* 1256, 1256–1263 (2023).

¹³ Information Technology Act, 2000 (Act 21 of 2000), s 67A; see also Avnish Bajaj v State (NCT of Delhi), 2008 (105) DRJ 721 (Delhi HC); State of Tamil Nadu v Suhas Katti (MM Court, Chennai, 2004).

Media Intermediaries to have a Grievance Officer, to receive complaints within twenty-four hours and resolve the complaints within fifteen days. While these steps can be seen as an advancement in terms of regulation, they have not been sufficient for tackling the problem of deepfakes.

b. The Bharatiya Nyaya Sanhita, 2023

The Indian Penal Code, 1860 was succeeded by the Bharatiya Nyaya Sanhita, 2023 (BNS) from 1 July 2024, which includes various provisions that can be used in cases where there is any harm caused due to deepfakes. Section 77 makes voyeurism an offence by making it unlawful to capture, publish or circulate any image of a woman performing a private act without her consent. Stalking is dealt with in Section 78 and also refers to stalking using digital or online mediums. Moreover, Section 79 prohibits publishing or transmitting any obscene content regarding women, whereas Section 96 deals with offenses related to child sexual abuse material.

One pertinent incident took place at the end of 2023 where the Government of India reacted to the rising concerns that were emerging due to the increasing number of deepfake incidents involving individuals of high stature. During November and December 2023, it issued notices for the intermediaries to adhere to their legal obligations of spotting deepfake material on social media platforms and removing them immediately. However, even though efforts have been made to regulate it, the BNS does not recognize the use of deepfake technology as an offense itself. Rather, it has to be brought to book using other laws.¹⁴

One major loophole in the law is the lack of a special law regarding the creation of these synthetic images without consent. It was stated in the 213th Report of the Parliamentary Standing Committee on Home Affairs concerning cyber crimes against women and children that technology outpaces legislation by a large margin. Hence, people who fall victim to this new form of cyber crime are at a disadvantage from a legal perspective.¹⁵

c. The Digital Personal Data Protection Act, 2023

The Digital Personal Data Protection Act, 2023 (DPDPA) is the first comprehensive law

¹⁴ Ministry of Electronics and Information Technology, 'Advisory to Intermediaries Regarding Deepfakes' (26 November 2023) available at: <https://meity.gov.in> (last visited on: May 26, 2026).

¹⁵ Parliamentary Standing Committee on Home Affairs, 'Cyber Crime Against Women and Children' (213th Report, Rajya Sabha, 2021) para 6.4 available at: <https://rajyasabha.nic.in> (last visited on: Jun 11, 2026).

enacted in India aimed at protecting personal data and outlines a set of duties and rights that can be used in the case of damage arising out of the misuse of deepfakes. The law defines personal data as any information concerning an identifiable natural person. Furthermore, processing of personal data should take place solely for the lawful purpose and should be done with the consent of the person whose personal data it is.

Nevertheless, the DPDPA cannot serve as a solution to deepfake abuse for several reasons. First, there is no private right of action under this legislation, as regulation and enforcement are entrusted to the sole discretion of the Data Protection Board of India. Also, the legislation is focused on imposing monetary sanctions and not criminal sanctions, which can decrease its deterrence factor, especially in cases where abusers act anonymously and do not have enough money to pay compensation. Additional limitations arise from exemptions made for such purposes as national security and law-enforcement activity. In addition, the manner in which the DPDPA will interact with the intermediary liability framework established under the Information Technology Act remains uncertain and awaits legal clarification.

d. Evidentiary Challenges

There are difficulties in prosecuting crimes associated with deepfakes due to the legal provisions for the admissibility and authentication of electronic evidences under Indian law. The provisions regarding electronic evidence have been incorporated in Section 63 of the Bharatiya Sakshya Adhiniyam, 2023, which replaces Section 65B of the Indian Evidence Act, 1872. In the case of *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, the Supreme Court of India laid down the legal requirements for admitting electronic evidences.¹⁶

The creation of deepfakes poses certain difficulties in the fulfilment of evidentiary standards in criminal cases. In view of the fact that the image/video created by means of deepfakes is a fake one, it should not only be certified to prove its authenticity but also be subjected to the forensic test in order to show that it was manipulated in terms of adding the face of the victim to another person's body. Though methods of detecting deepfakes have significantly improved, their reliability is far from being absolute. At the same time, there is no established judicial practice in India in terms of evaluation of forensic results concerning deepfake evidence. Given the fact that proving the guilt is the prosecutor's burden, forensics will necessarily require an

¹⁶ *Arjun Pandit Rao Khotkar v Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1; see also *Anvar P.V. v P.K. Basheer*, (2014) 10 SCC 473.

expert opinion.¹⁷

4. Comparative Perspectives

a. The United States

Whereas a specific set of federal guidelines to counter illegal generation of intimate images using AI was only recently developed, there have been efforts to tackle deepfake related problems in the USA via state and federal legislation. For example, California introduced some laws governing the content in question. In 2019, it enacted Assembly Bill 602, which gives people the right to bring a civil lawsuit against any deepfake pornographic content that caused them any harm, as well as Assembly Bill 730, which prohibits the use of manipulated audio-visual content in order to sway the elections. Meanwhile, in the same year, Virginia updated the relevant part of the criminal code, Section 18.2-386.2, criminalizing non-consensual deepfake pornography.

An important development at the federal level is the enactment of the DEFENDING ACT (Defining Electronic Frontier Action for Non-Consensual Intimate Visual Depictions) in 2024. The DEFENDING Act provided a uniform civil solution for individuals whose rights have been violated due to non-consensual intimate visual depictions, which may have been created through artificial intelligence. The international character of the distribution online and the interstate issues of the harm caused by the use of technology highlight that state regulation is insufficient.

b. The European Union

However, the EU has employed a wider regulatory framework to tackle the danger posed by deepfakes since they have assigned many duties to the platforms functioning within the digital single market in Europe. As per the Digital Services Act (DSA), which came into full force in February 2024, the very large online platforms have to assess the systemic risks that emerge from their services, which includes technology-mediated gender-based violence, and mitigate such risks. Instead of making deepfakes an offense under the law, the DSA mandates the platforms to have certain policies regarding the management of non-consensual intimate

¹⁷ R v. Sharpe, [2001] 1 SCR 45.

images using synthetic media technology.¹⁸

EU's AI Act, adopted in 2024, is an important step forward in regulating deepfakes due to the introduction of particular requirements concerning transparency. According to Article 50, creators of AI systems, which can generate synthetic media, should provide for the presence of machine-readable indicators allowing the detection of these outputs as deepfakes. Moreover, in case deepfake media becomes available to the public, people who use this media need to be informed about the artificial nature of it. Besides these measures, biometric data, which can also be used for generating deepfakes, can be considered special categories of personal data under GDPR and its processing requires consent from the data subject.¹⁹

Although the Council of Europe's Istanbul Convention on Prevention and Combating Violence Against Women and Domestic Violence does not refer to the use of deepfakes technology, its provisions offer a solid legal framework for considering the creation of non-consensual synthetic pornographic material as a form of gender-based violence. It has been emphasized in a UN special rapporteur report on violence against women and girls released in 2023, which urged states to adopt legislation to regulate AI-enabled gender-based violence and protect the rights and interests of women and girls in doing so.²⁰

5. Constitutional Dimensions

a. The Right to Privacy

The constitutional justification for legislating protective measures to protect people against damage resulting from deepfakes is very well established in the case law of Indian jurisprudence, especially in light of the recent judgment by the Indian Supreme Court in the case of *K.S. Puttaswamy (Retd.) v. Union of India*. In this judgment, the Supreme Court, through a unanimous judgment of a nine-judge Constitution Bench, held that privacy is an integral part of the fundamental rights to life and liberty guaranteed under Article 21 of the Indian Constitution.²¹

¹⁸ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act) [2022] OJ L277/1, Arts 34 and 35.

¹⁹ See AI Act (Regulation (EU) 2024/1689 of 13 June 2024 on Artificial Intelligence), Art 50; see also Recitals 133-134 on deepfakes and transparency obligations for AI-generated content.

²⁰ United Nations Special Rapporteur on Violence against Women and Girls, Report on Technology-Facilitated Gender-Based Violence (A/HRC/53/35, 2023) paras 22-28.

²¹ *K.S. Puttaswamy (Retd.) v Union of India*, (2017) 10 SCC 1.

The creation of a deepfake image of a woman without her consent amounts to an evident violation of informational privacy. This act entails the use of her personal characteristics such as facial appearance without her consent or approval. The act is carried out in an environment beyond her control and is done with the intention of inflicting damage on the person. Privacy rights guaranteed under Article 21 of the Constitution as upheld in the case of *Puttaswamy v Union of India* are not just a negative right of the state to stay away from interfering in people's lives but also entail a positive obligation to enact laws that will protect people from any privacy violation done by non-state actors.²²

b. The Right to Dignity

Deepfake technology also poses many threats to the constitutional guarantee of human dignity, which has been considered by the Supreme Court to be an inherent part of the fundamental right to life guaranteed under Article 21 of the Indian Constitution. While dealing with gender-based violence and sexual harassment cases, in the case of *Vishaka vs. State of Rajasthan*, the Supreme Court read into Articles 14, 19, and 21 of the Constitution to ensure that women have the right to live and work in circumstances where there is no threat to their dignity. Creation and distribution of synthetic pornographic material without the consent of the person involved is a serious violation of this right, the seriousness of which cannot be contained within the parameters of obscenity or voyeurism.²³

The point made here is that in order to respect the constitutional dignity principle, the non-consensual use of a person's identity for sexual abuse or degradation must be established as a specific criminal act by statute. The significance of recognizing this behavior as a separate wrong goes well beyond any legal implications.

c. Freedom of Speech and the Question of Balance

One of the most important issues in formulating a deepfake bill is striking the appropriate balance between protecting women from technology-induced harm and maintaining the core value of freedom of expression guaranteed under Article 19(1)(a) of the Indian Constitution. Artistic expression, which includes satirical or parody expression of personalities and artists,

²² *Puttaswamy v Union of India*, (2017) 10 SCC 1.

²³ *Vishaka v State of Rajasthan*, AIR 1997 SC 3011; *Apparel Export Promotion Council v A.K. Chopra*, AIR 1999 SC 625.

is constitutionally protected and should not be overly burdened. Therefore, a broad and all-encompassing deepfake bill will run the risk of regulating free and legitimate expression, which may not necessarily be illegal and harmful.

One of the landmark judgments of the Supreme Court of India in this regard is the judgment in *Shreya Singhal v. Union of India*. In that case, Section 66A of the Information Technology Act was struck down for being overly vague and broad, which could result in curtailing freedom of expression. Thus, any legal framework concerning deepfakes must clearly delineate the types of content that are liable for legal action. It is important to make a differentiation between those pieces of content that have the direct infringement on the rights of individuals, like the creation of sexual content without consent, and those pieces of content that might mislead people but do not create an individual-specific problem. Well-defined offences, proper definition of criminal intent, and effective judicial supervision are crucial for avoiding the discouragement of legitimate activities through regulation.

6. Conclusion

The use of AI technology to create and distribute fake images of women constitutes a serious and developing issue of cyber harassment that calls for immediate and carefully crafted legal responses. While India presently makes use of the provisions of the Information Technology Act, 2000, Bharatiya Nyaya Sanhita, 2023 and the Digital Personal Data Protection Act, 2023 to tackle online abuses, none of these laws is fit to counter the phenomenon of deepfake abuse. Their provisions are either too narrow in scope, inadequately addressing deepfake issues or rely heavily on ex post facto measures.

A robust constitutional grounding for regulating this emerging technology exists. Constitutional rights to privacy and human dignity recognized in the *Puttaswamy* judgment combined with subsequent case law on violence and discrimination against women clearly justify legislative action in this area. An examination of regulatory practices abroad shows that merely resorting to criminal punishment will be insufficient. The combination of criminal, civil and other types of measures could significantly mitigate the harm caused by deepfake abuse without running contrary to constitutional protection of freedom of speech.

Recognition of this problem legally requires more than just criminalizing any wrongdoing. It is also important to ensure that adequate remedy is provided to victims through means that are

practical, speedy, and accessible. Though there is still much work to be done in terms of enacting proper legislation, the constitutional basics needed for that have already been laid down.

REFERENCES

1. Citron D.K., *Hate Crimes in Cyberspace* (Harvard University Press 2014).
2. Citron D.K. and Franks M.A., 'Criminalizing Revenge Porn' (2014) 49 *Wake Forest Law Review* 345.
3. Goodfellow I. and others, 'Generative Adversarial Networks' (2014) 27 *Advances in Neural Information Processing Systems* 2672.
4. Ajder H. and others, 'The State of Deepfakes: Landscape, Threats, and Impact' (Deeptrace, 2019).
5. National Crime Records Bureau, *Crime in India 2022* (Ministry of Home Affairs, New Delhi, 2023).
6. National Commission for Women, *Annual Report 2022-23* (NCW, New Delhi, 2023).
7. Parliamentary Standing Committee on Home Affairs, 'Cyber Crime Against Women and Children' (213th Report, Rajya Sabha, 2021).
8. UN Special Rapporteur on Violence against Women and Girls, *Report on Technology-Facilitated Gender-Based Violence* (A/HRC/53/35, 2023).
9. Ministry of Electronics and Information Technology, *Advisory to Intermediaries Regarding Deepfakes* (November and December 2023).
10. R. Ranjan, "Navigating the Digital Frontier: The Intersection of Technology and Criminal Liability in Modern Jurisprudence" in Abhijit B. & Sajal Sharma (eds.), *Disruptive Technologies and the Law: Navigating Legal Challenges in an Era of Innovation* 41, 41–48 (Iterative International Publishers (IIP), 2024).