
NON-CONSENSUAL DEEPFAKE SEXUAL CONTENT: PRIVACY, CONSENT, AND GENDERED HARMS IN THE DIGITAL AGE

Gaurav Kumar Yadav, PhD Research Scholar, School of Law, Mahindra University

Madabushi Venkata Vasudev, PhD Research Scholar, School of Law, Mahindra University

Dr. Rishi Raj Bhardwaj, Assistant Professor, School of Law, Mahindra University

ABSTRACT

The new ripple of AI has brought about deepfake technology, which assists in the creation of super-realistic not just audio-visual but also fake information. Even though there are few landscapes where deepfake are recognized, their illicit application has turned into key kinds of image-based sexual abuse, specially about the non-consensual, AI-created sexual content. The present research examines the deepfake sexual violence as a gendered harm and places in the larger framework of digital discrimination, patriarchy, and cybercrime. It points out that the abuse of deepfakes, which mainly targets women, not only reinforce but also give life to old age control system over women's bodies, sexuality, and digital identities. This study contemplates to address the problem of power exertion, retaliation, sexual exertion, and infringement of consent as intention of perpetrator by taking doctrinal and analytical facets, which is supported by feminist theory. In addition to study similar regulations like GDPR, and global ethical norms such as UNESCO's recommendations on ethics of AI, the study severely examines the India's legal approach under the Information Technology Act 2000, and the Digital Personal Data Protection Act 2023. The study exposes the numerous crucial legal gaps, involving absence of particular laws regulating deepfakes, unclear designation of intermediary responsibility, and the limited method of enforcement. The study bestows the accurate information about grave moral concerns that are originated as a result of deepfakes sexual assault as a violation of consent, autonomy, privacy, dignity and right to be forgotten. Ahead, of this victim faced "social, psychological and reputational harm, and loss public trust in digital media. Thus, it concludes that India's current legal system and moral system are insufficient to tackle with the problems of deepfake sexual abuse which is characterized as a huge scale diffusion, anonymity, and precipitate of internet. Also, it stresses on the, there should specific legislation on Deepfakes sexual abuse, greater platform and intermediaries' liabilities, victim centric approach etc.

Keywords: Deepfakes, UNESCO, DPDP ACT, IT ACT, Public Trust, GDPR

INTRODUCTION

“Power is fragmenting women’s bodies into pieces and merging them into new objects for male desire.”¹

Cybercrime has become a key concern in the modern time of digitalization and technology. Cybercrime is characterized as being distinct from other crime as it takes place online. Cybercrime is defined as illegal acts or crimes committed via the use of the internet and information and communication technologies.² There is currently no accord on what formed cybercrime, albeit experts have tried to define it. This general term usually encompasses a diversity of digital crimes.³ Cybercrime is a term used by governments, the business community, and the general public to depict a diversity of illegal acts and practices including computers, the Internet, or other technological equipment.⁴ Our society has witnessed growth that offer amazing possibility for progress in an era of eccentric technological breakthroughs. Unfortunately, despite this incredible growth, we are encountered with the harsh reality that the very technologies advancing humanity forward are also inflicting grave harm on those around us. The quick diffusion and creation of deepfakes represent one of the most alarming growths in this technology. The term deepfake refers to the creation of fake pornography by using deep learning technology to superimpose one person’s face onto another person’s body in photos or videos. The elements of the word deepfake themselves define it: deep refers to deep learning, and fake means deceptive or misleading.⁵ The growth of GANs- networks used for machine learning algorithms-led to the origin of deepfake technology in the mid-2010s. A usual method is used to collect data, train the model, and amend and refine the content to create deepfake material.⁶ In year 2017, a Reddit user used this technique to change the faces of adult film stars with the faces of celebrities, giving rise to the term “deepfake.”⁷ Deepfake videos,

¹ Hass A, “Virtual Illusions: A Legal and Gendered Analysis of Deepfake Sexual Abuse” [2025] Master’s Thesis Submitted to the department of Criminology, The University of Auckland.

² Karuppannan J, “Cyber Criminology and Space Transition Theory: Contribution and Impact” (2025) 12 SSRN Electronic Journal

³ Sabillon R and others, “Cybercriminals, Cyberattacks and Cybercrime,” “2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)” (IEEE 2016) <https://doi.org/10.1109/icccf.2016.7740434> accessed December 9, 2025

⁴ Wall DS, *Cybercrime: “The Transformation of Crime in the Information Age”* (Cambridge: Polity Press 2008)

⁵ Heidari A and Jafari Navimipour, “Deepfake Detection Using Deep Learning Methods: A Systematic and Comprehensive Review:” (2023) 14 WIREs Data Mining and Knowledge Discovery

⁶ Chesney R and Citron DK, “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security” (2018) 107 SSRN Electronic Journal 1753

⁷ Badshah N, “Nearly 4,000 Celebrities Found to Be Victims of Deepfake Pornography” *The Guardian* (March 21, 2024) <https://www.theguardian.com/technology/2024/mar/21/celebrities-victims-of-deepfake-pornography> accessed December 11, 2025

ranging from false speeches by Barack Obama to claims and held responsible to Mark Zuckerberg that “Facebook misuses user data and infringe privacy, have become speedily usual.” These videos are about impossible to find out as fake, making it easy for viewers to be deceit into believing they are original.⁸ The caliber to easily manipulate information using deepfakes has taken a hazardous turn, making AI-generated image-based sexual assault, a new form of digital sexual abuse, possible. Digital sexual harassment is naturally gender-based, as evidenced by the disproportionate number of women among victims of “cyber abuse 99% of victims of deepfake sexual abuse are women, and 57%” of people globally have reported being victims of image-based sexual abuse.⁹

While these data are alarming, they are not surprising, as men have historically controlled and oppressed women and their bodies. The patriarchal structures that assist, encourage, and profit from the ignorance of women are at the root of deepfake sexual abuse. Post-structural feminists use recitation analysis to question prevalent myths about identity, agency, and the body. The purpose of bug bounty programs on social media sites like Facebook is to search path to identify deepfake content. Usually, deepfakes are software tools rooted on machine learning that create artificial media that it shows realistic.¹⁰ These social manners really benefit from and perpetuate the ignorance and exploitation of women. Controlling women’s bodies and sexuality is nothing new, even without deepfakes. By decreasing women to their body parts and changing them into virtual objects for male satisfaction, they bar women of their humanity and agency. These problems go ahead of mere sexual images. It is kind of cybercrime which occurs against the Indian women.¹¹ It has not defined clearly in any statute in India till now. Which leads a legal gap in framework deepfake technology can be used for blackmailing, harassing and defaming the women. Deepfakes have a far deeper cultural influence on Indian women than just personal strain. For example, this type of manipulated media can create an environment of suspicion about the integrity of information and images, making it even tough to understand and it is hard to find that whether one is in coeval with another rights, reform among the sexes is a huge gap, all due to their becoming womankind and deepfakes can make their lives even

⁸ Silverman C, “How To Spot A Deepfake Like The Barack Obama-Jordan Peele Video” *BuzzFeed* (April 17, 2018) <https://www.buzzfeed.com/craigsilverman/obama-jordan-peelee-deepfake-video-debunk-> accessed December 11, 2025

⁹ “TFGBV: Deepfakes and Image-Based Abuse” (Office for the Prevention of Domestic Violence) <https://opdv.ny.gov/tfgbv-deepfakes-and-image-based-abuse> accessed December 11, 2025

¹⁰ Laffier J and Rehman A, “Deepfakes and Harm to Women” (2023) 3 *Journal of Digital Life and Learning* 1

¹¹ Rini R and Cohen L, “Deepfakes, Deep Harms” (2022) 22 *Journal of Ethics and Social Philosophy*

worst. This will negatively influence women's self-confidence, mental health, and overall well-being.¹²

IMAGE BASED SEXUAL VIOLENCE & MOTIVATION OF OFFENDERS

When we ponder sexual violence, we oft think about a condition where physical violence is used to force someone to satisfy sexually, mainly by means of rape or sexual assault. Albeit, this is indeed a form of sexual violence that we will not elaborate on since topic is distinct, it is just one of many facets of the issue it is a more deceptive form of sexual abuse has raised in the digital world, one that is easily repeated and causes excessive damage to the victim. This type of sexual abuse is called image-based sexual abuse, and it includes the creation, dispensation, and demonstration of sexually explicit images in absence of consent.¹³ If we look traditionally, women and girls have been the primitive victims of sexual abuse. Deepfakes are being used to injure women in new ways, and there appears to be no limit to their abuse. Deepfakes have given the term sexual abuse a new meaning. Thanks to deepfake technology, sexual abuse is expanding continuously in both society and the digital world. This sort of abuse is oft expanding via text messages, emails, social media, and even face-to-face encounters.¹⁴ Because enactments addressing non-consensual deepfake photos and image-based sexual abuse are still being evolved, numerous victims feel unsafe and believe the government is failing to safeguard them. In pursuance to UK guidelines on image-based sexual abuse and revenge pornography, an offense is only pondered to have occurred if the intention behind sharing the image or video was to trouble the person shown. Likewise, promulgating a private sexual image in absence of the assent is only illegal if the aim is to trouble the person depict in the picture who did not permit to its sharing. For example, if the content was shared because it was pondered comical, it would not be illegal. Under such laws, proving crime for both the victim and the offender is very hard. As a result, image-based sexual assault can keep on without any meaningful outcome.¹⁵ Even albeit there an oft connection made between the offenders and reasons of their action, the list of relation is not all inclusive. At the same time,

¹² Coffin J, "Asking Questions of AI Advertising: A Maieutic Approach" (2022) 51 Journal of Advertising 608

¹³ Ringrose J and others, "Young People's Experiences of Image-Based Sexual Harassment and Abuse in England and Canada: Toward a Feminist Framing of Technologically Facilitated Sexual Violence" (2022) 93 Women's Studies International Forum 102615

¹⁴ Henry N, Flynn A and Powell A, "Policing Image-Based Sexual Abuse: Stakeholder Perspectives" (2018) 19 Police Practice and Research 565

¹⁵ Okolie C, "Artificial Intelligence-Altered Videos (Deepfakes), Image-Based Sexual Abuse, and Data Privacy Concerns" (*Virtual Commons - Bridgewater State University*) <https://vc.bridgew.edu/jiws/vol25/iss2/11> accessed December 13, 2025

we won't engrossed into distinct cases of sexual assault in exhaustive. Sex perpetrator commonly has bad motive which are connected to the way which are linked to the way they would like to be felt. But there are many incidents where friends and family members are do such crime without any motive at all. The study conducted by Vasiliya Karassava and Adele Forth in year (2022) in this report they demonstrate the "*data that about 56.9% of this kind of abuse*" victims focused close or former partners as abusers. Ahead, more than "*half 64.3% of participants depicts that the abuser was someone they know or their relative albeit, 15.9%*" of respondent declared that they were not able to recognize the abuser.¹⁶ This points out that the reason behind image-based abuse can be very diverse, involving among others, sexual pleasures, and consent of total strangers, and revenge via individual offenders like ex-lover, or upset relatives. The key reasons why people commit image-based abuse are listed below-

- **Sexual Pleasure and Bullying via Power Exertion**

This is the one of the key reasons for sexually abusive behavior via images is the longing of people to please themselves either by psychologically or physically provoking their senses. And the key cause for image-based sexual abuse is the abuser desire's to emotionally and psychologically overpower the victim via constant abuse just to depicts that he or she can (or has the authority or competence) to particularly with the goal of winning the victim. Researchers such Anastasia Powell & Nicola Henry in year 2019, guessed that image-based sexual violence is just one facets of larger spectrum of the gendered-based intimate partner violence, and that it might outcome that the intimidating nature of behavior becomes more blend of pattern influence and coercive control.¹⁷ The offender uses the Deepfake technology to intimidate, blackmail, and abuse their victims in domestic violence cases, which makes deepfakes technology a grave risk for them.¹⁸

- **Circumventing Consent**

Distinct from other kind of sexually abusive to few extents, given the absence of

¹⁶ Karasavva V and Forth A, "*Personality, Attitudinal, and Demographic Predictors of Non-Consensual Dissemination of Intimate Images*" (2021) 37 Journal of Interpersonal Violence NP19265

¹⁷ Nicola Henry, Flynn A and Powell A, *Image-Based Sexual Abuse: Victims and Perpetrators* (Australian Institute of Criminology 2019) <https://doi.org/10.52922/ti09975> accessed December 31, 2025

¹⁸ Lucas KT, "*Deepfakes and Domestic Violence: Perpetrating Intimate Partner Abuse Using Video Technology*" (2022) 17 Victims & Offenders 647

agreement being the makers of such image-based sexual content, if in any instance linked with deepfakes are driven by the desire for the experience to simulation via AI-done videos and they like not to ask for the consent and get the consent.¹⁹

- **Revenge**

Revenge is the term used for support the aggression as a response to willful injury prone. Such action has characterized by the counterattack overtly focused at the bad or the object of the force, normally in retaliation for an injury or an injustice that the victim either has experienced or think he/she has experienced at the hand of aggressor. One such way of infringing the right is via the act of revenge porn, which includes the sharing of private pictures without the individual consents. An aggrieved person, an ex-intimate partner, or anyone who has seen or has accessed to victim explicit content can be the offender of image-based sexual assault. The wrongdoer in question makes in use of this material only for the aim of inflicting the victim's pain, or ruining the victim's image in society or defeating the victim via controlling the victim.²⁰ Revenge on an ex-partner, who choose for the break-up may be the reason for non-consensual diffusion of someone's intimate pictures and videos particularly if the offender is otherwise inhibit from physical interaction with the victim. The main goal of the offender to balance the matter make the offender to be feel the same pain and teach them same lesson.²¹

- **Sextortion**

The Cambridge University in 2022 give bestow definition on Sextortion; it is crime conducted via the internet where a person generally employed in few sorts of sexual activity, is forced to do it, under the intimidation of exposing nude pictures, or intimate content. It is kind of coercion including the forced diffusion of explicit images, private or otherwise, or even the most commonly of the case, the abuser receiving more of such images, sex acts, or monetary profits. "*Female victims of image-based sexual abuse*"

¹⁹ Flynn A, "Inside the Minds of Deepfake Abusers: What Drives AI-Fuelled Sexual Abuse?" *Monash Lens* (December 3, 2025) <https://lens.monash.edu/inside-the-minds-of-deepfake-abusers-what-drives-ai-fuelled-sexual-abuse/> accessed January 1, 2026

²⁰ Mania K, "Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study" (2022) 25 *Trauma, Violence, & Abuse* 117

²¹ Dyduch-Hazar K and Mrozinski B, "The Satisfaction Is Mine: Revenge Seeking Following Extrinsic Reward" (2022) 163 *The Journal of Social Psychology* 52

can be intimidated with the diffusion of their explicit content or images, videos if they decline to pay or to have sex with the offender.²²

ARTIFICIAL INTELLIGENCE-GENERATED DEEPPAKES: A NEW THREAT TO GENDER SAFETY

The underlying idea behind the digitalization is to reform the quality of life of people, but it is women who suffer most from the less than legitimate distribution benefits cause from these changes.²³ The gender gap in access to, participation in, and outcome of the digital technologies is the global incident. The double disaster of gender and race and class or sexual orientation or ethnicity creates particular situations for women living in poor communities. Such biases are not existing but also predominate via the very nature of data-driven system and algorithms despite their claims of objectivity. The situation is made even worse by lack of representation of women and other marginalized group in tech leadership, which permits AI to intimate and magnify the existing social injustices over time.²⁴ The key goal of artificial intelligence to solve the problem that are complicated and hard to handle and that needs the processing of techniques applicable to both man and machine. The criminal relies more and more on AI to contemplate and enhance their attacks in the electronic world, targeting not just individual but also targeting to government and companies. Albeit, the world of criminals has not depicted much of their expertise in handling the system. They completely aware of the dark capability of AI and machine learning system.²⁵ The present shifts in the market depict that malware creation and diffusion along with ransomware attacks are being speedily conducted over the internet, with AI playing a key role in speed, size, and effectiveness of these cybercriminal operations.²⁶ AI-created deepfakes have change out to be broadly recognized technique of online maltreatment which cut athwart numerous sectors. Deepfakes work by using a combination of neural networks and deep learning algorithms to create enormously realistic imitations of real people's voices, faces, and videos based on the processing of huge

²² Patchin JW and Hinduja S, "Sextortion Among Adolescents: Results From a National Survey of U.S. Youth" (2018) 32 Sexual Abuse 30

²³ Wajcman J, Young E and Fitzmaurice A, *The Digital Revolution* (United Nations 2020) <https://doi.org/10.18356/e2a68ccf-en> accessed January 2, 2026

²⁴ Wajcman J and Young E, "Feminism Confronts AI, Feminist AI" (Oxford University PressOxford 2023) <https://doi.org/10.1093/oso/9780192889898.003.0004> accessed January 2, 2026

²⁵ Khanna P and Khanna R, "Artificial Intelligence and Cybercrime-A Curate's Egg" (Medium, June 14, 2020) <https://medium.com/the-%C3%B3pinion/artificial-intelligence-and-cybercrime-a-curates-egg-2dbae833be1> accessed January 2, 2026

²⁶ Velasco C, "Cybercrime and Artificial Intelligence. An Overview of the Work of International Organizations on Criminal Justice and the International Applicable Instruments" (2022) 23 ERA Forum 109

data set. Albeit this technology claims to have good applications, it is gradually being used for illegal gain such as impersonation, emotional torture, blackmail, and bias, specially directed women and the youth.²⁷ Deepfakes are ponder a novel method of image-based sexual abuse that can inflict grave harm in physical, social, and psychological and reputational facet. They are often employed as a means to control, scare, and insulting women.²⁸

The deepfake pornography is likely to directed at women rather than men, as per the Amsterdam-based cyber security firm, Deep trace, increase in the discrimination against the female gender. Women almost for 90% of victim of “*revenge porn, non-consensual porn, and distinct form of harassment;*” deepfake is just another case. So, the use of Artificial Intelligence is creating deepfakes will becomes a normal thing as the trends goes. Deepfake are the artificial media produced by the Artificial Intelligence that change the person’s video or photo with their own. However, the key issues with the deepfakes are their much high level of realism, which oftentimes makes is almost impossible to tell the which media is original and which media is altered or fake. Apart from this, they possess both real and probable capabilities to misguide, manipulate, and deceive people via the diffusion of misinformation, propaganda, fraud, extortion, and creating fake identity.²⁹ In the event that this trend keep maintained, deepfake the manipulation of digital content by means of deepfake technology will no doubt to become one of the facets of AI usage. Deepfakes consists of AI algorithm that “*superimpose someone’s face over an existing video or image.*” The problem with deepfake is that they look completely so real that it is really difficult for the anyone to tell the which media is manipulated and which is real one. On top of this, they have real capacity to, spread lies, deceit, blackmail, and influence and imitation. To illustrate, there is a latest scandal of AI-generated sexual visual of Actress Taylor Swift was able to “*attract more than 45 million views, gets 24,000 reposts and receive hundreds of thousands of like and bookmarks*” during the almost 17 hours that it was display before being taken down. It was finally done away with, but not before the image became popular and spread via social media and user profiles, this cause great damage.³⁰ The

²⁷ Henry N and others, “*Image-Based Sexual Abuse,*” “*Image-based Sexual Abuse*” (Routledge 2020) <https://doi.org/10.4324/97811351135153-1> accessed January 2, 2026

²⁸ Dunn S, “*Technology-Facilitated Gender-Based Violence: An Overview*” (Centre for International Governance Innovation, December 7, 2020) <https://www.cigionline.org/publications/technology-facilitated-gender-based-violence-overview/> accessed January 2, 2026

²⁹ Ajder Henry and others, “The State of Deepfakes: Landscape, Threats, and Impact” [2019] Deeptrace, Amsterdam, <https://docslib.org/doc/12559428/the-state-of-deepfakes-landscape-threats-and-impact-henry-ajder-giorgio-patrini-francesco-cavalli-and-laurence-cullen-september-2019>, accessed January 1, 2026

³⁰ Schmunk R, “*Explicit Fake Images of Taylor Swift Prove Laws Haven’t Kept Pace with Tech, Experts Say*” (CBC, January 26, 2024) <https://www.cbc.ca/news/canada/taylor-swift-ai-images-highlight-need-for-better-legislation-1.7096094> accessed January 1, 2026

use of deepfakes leads to excessively risky in online setting that objectifying women's bodies in the digital form, and pictures are tempered with or fun without their permission. The cybersecurity firm Sensity, put emphasis on that the deepfake material increase on large scale, and it is doubling roughly every half a year. Out of 85,000 fake films that are available online, almost "90% depict women who are not allow it to participate in production of pornographic content." The creator of such content is in distinct parts of the world; analyzing the most visited deepfake sites expose that the creators are from the India, Guatemala, U.S., Canada and other places.³¹

LEGAL AND JUDICIAL PERSPECTIVE

The elementary law that controls Deepfakes-related crimes in India is "*Information and Technology Act 2000*," which is the most crucial legislation in this area. Crimes like "*computer impersonation, cheating are covered under section 66D*," which also involve coercion and fraud based on Deepfake.³² Invasion of privacy is dealt with section 66E via the prohibition of taking, publishing, or transmitting, private photographs or videos without the consent. Overall, all these provisions offer a means of handling the wrongful use of Deepfakes in terms of deceit, invasions of privacy, and misuse of technology.³³ The IT Act deals with the issue of Deepfakes depicting sexual or pornographic content via section 67A and 66B, Which set forth the penalties for the publication, distribution of sexually explicit materials including adults and children.³⁴ As, consequence of these regulations, a "*number of sites, among them Pornhub, absolutely banned the use of Deepfake technology for sexual purpose*." Moreover, section 79 lays down the rules for intermediary liability, which needs that websites that contain deepfake content must take down illegal materials after they get actual knowledge or receive court order to remove it.³⁵ In the case of "*Myspace Inc. V. Super Cassettes Industries Ltd.*"³⁶ in this case court held that even without the court order, intermediaries are still bound to remove the violated content as soon as they notified. The IT Act 2000, change the whole "*scenario for big social media intermediaries*" making it hard for to adhere with these new rules as it wants compliance officer, content monitoring, and tracing of information source. The new regulations

³¹ Compton S, "What Are Deepfakes? More and More Women Are Facing This Form of Online Abuse" *Vogue* (March 16, 2021) <https://www.vogue.com/article/scary-reality-of-deepfakes-online-abuse> accessed January 2, 2026

³² Information Technology Act 2000, S. 66D

³³ Information Technology Act 2000, S. 66E

³⁴ Information Technology Act 2000, S. 67A, & S. 66B

³⁵ Information Technology Act 2000, S. 79

³⁶ *Myspace Inc. V. Super Cassettes Industries Ltd.*, (2016) Delhi High Court, 8178- DB

also bestow a mechanism for settlement of grievances whereby consumer complaints are taken care of. Still, the outlined observance and surveillance practices may be violated upon the “right to privacy which is protected under Article 21” of the Constitution of India as per the judgment of “*Justice K.S Puttaswamy V. UOI.*”³⁷ Ahead, the use of people’s images for deepfakes without their consent is clear infringement of their fundamental right to privacy.

DIGITAL PERSONAL DATA PROTECTION ACT 2023 & RIGHT TO BE FORGETTEN

Before the “*passing of DPDP Act 2023*,” India was mainly governed by the IT Act, 2000, which was piece of legislation focused mainly at electronic transactions; it also handled the few issues of data protection.³⁸ “*The adoption of GDPR as a model for DPDP Act 2023*” signifies a valuable step in the modification of the digital personal data processing. Its application is, still, limited since it not covers the international corporations that track the business outside of India.³⁹ The Act, while not endowing the authority for making rules or giving guidance, outlines the individual data rights, introduce the notion of purpose limitation, and sets up the Data Protection Board for handling the complaints and the impositions of penalties.⁴⁰ The law mainly concerns about the foreign legal system that process digital personal data in India for the goal of giving or selling services to the data subjects.⁴¹ But, since the wording on the issue of the conduct tracking was not involved in the final document, the range of application is still undefined. This opacity is problem when talking about international companies that track the internet usage of Indian people and law’s coverage of them.⁴² The DPDP Act does not specifically outline AI-created content, but still, responsibilities of data fiduciaries can be applied to deepfakes. The DPDP has an extremely lot to say about data accuracy and perfectness, especially if the data impact a data principal, as per the section 8(3),⁴³ there is need while section 8(5)⁴⁴ calls for deletion of info produced by unlawful AI upon

³⁷ Justice K.S Puttaswamy V. UOI, (2017) 10 SCC 1 (SC)

³⁸ Digital Personal Data Protection Act 2023

³⁹ Kanoongo A and Adari H, “*Unpacking India’s Digital Personal Data Protection Act: A New Dawn or a False Start?*” (OHRH) <https://ohrh.law.ox.ac.uk/unpacking-indias-digital-personal-data-protection-act-a-new-dawn-or-a-false-start/> accessed January 3, 2026

⁴⁰ Digital Personal Data Protection Act 2023, S. 18

⁴¹ Digital Personal Data Protection Act 2023, S. 3(b)

⁴² Dorwart H, Gallan J and Hammachi VR, “*Decrypting India’s New Data Protection Law: Key Insights and Lessons Learned*” (Bird & Bird, October 13, 2023)

<https://www.twobirds.com/en/insights/2023/global/decrypting-indias-new-data-protection-law-key-insights-and-lessons-learned> accessed January 3, 2026

⁴³ Digital Personal Data Protection Act 2023, S. 8(3)

⁴⁴ Digital Personal Data Protection Act 2023, S. 8(5)

finding. The *devoir* connected to data safety also invoked in the case of deepfakes when they are used for predictions and marketing; the term “likely” does the trick. Ahead, section 7 talks about explicitly collected consent in the case of personal data so that the data cannot be used, and thus easily framed in the training of generative AI models particularly by social media platforms.⁴⁵

The DPDP Act 2023, in its section 12, the “*right to be forgotten*” support the duty of data fiduciary to eliminate harmful material such as deepfakes. This right also recognized by Article 17(2) of GDPR, underlines the necessity to find the middle ground among personal privacy and freedom of expression. This ruling in “*Google Spain SL Google Inc. V. AEPD, Mario Costeja Gonzalez*”,⁴⁶ serves as example of how weighing “*public interest against the sensitivity and influence of personal data*” in central premise of European Law. In the earlier case of **Zulfikar Ahman Khan & Mahendra Kumar Jain**,⁴⁷ Indian Courts also recognized “*the right to be forgotten as a perspective of Article 21*” thus enhancing the data fiduciary duty to assists victims of deepfakes. A public interest litigation filed in the case of **Chaitanya Rohilla V. Union of India**⁴⁸ regarding the unregulated “*use of deepfakes and AI technologies was brought*” to the Delhi High Court. The court pointed out that necessity of weighing and carefully pondering the distinct interest before the government, which has maintained that the issue highlighted are already being handled via the legal framework and the DPDP Rules 2025, which has supplemented the DPDP Act 2023 thereby strengthening the regulatory framework, intervened, Rule 3 requires informed and transparent consent, Rules 6 command the implementation of suitable security measures such as masking and encryption; Rule 7 impose harsh 72 hours reporting timelines for data breaches; Rule 4 introduces consent managers. The overall result of these regulations is the growth of accountability and the intricacies of the personal data to create deepfakes.⁴⁹

ETHICAL CONSIDERATIONS

The use of deepfakes technology online, besides bringing about a valuable blow to the integrity of information, raises a host of ethical issues linked to consent, autonomy, privacy, and power dynamics. It erases people’s control over the digital identities, images, likability or it simply

⁴⁵ Digital Personal Data Protection Act 2023, S. 7

⁴⁶ Google Spain SL Google Inc. V. AEPD, Mario Costeja Gonzalez, (case C-131/12) EU:C:2014:317

⁴⁷ Mahendra Kumar Jain v. State of W.B, WPA No. 17293 of 2021(Cal HC)

⁴⁸ Chaitanya Rohilla V. Union of India, WP (C) 15596/2023, CM APPL. 62399/2023

⁴⁹ Digital Personal Data Protection Act 2023, Rule 3, 4, 5, 6, 7

takes away their control over their whole online persona. This is particularly true in India, where the use of deepfakes is in direct infringement of the *"fundamental rights to life and personal liberty,"* which was enshrined in *"Article 21 of the Constitution of India and which has been interpreted in case of Justice K.S Puttaswamy V. Union of India."* the usage of AI in India is governed by only some of the principles such as responsibility, transparency, human dignity, and non-harm that were highlighted in *"UNESCO's 2021 recommendation on Ethics of AI"*. Deepfake are the cause of mental suffering, psychological distress, and damage one's reputation, particularly via the non-consensual and virtually simulated sexual content that is most harmful.⁵⁰ The deepfake technology deeply *"influenced the women who has been subjected to online abuse"* and they reinforce the patriarchal power system, as they are one mostly affected by the creation of non-consensual sexual images. Such practices are direct infringement of human dignity and freedom of communication via the information since they take away the *"control of identity and physical appearance"* from the people worried. The negative results of these practices go beyond the individual suffering, though; the whole society trust gets undermined, women get excluded from public life, and the internet is becoming a more misogynistic place as a result. Thus, the requirement for the ethical framework in the AI-Governance which includes, *"transparency, accountability, consent-based data use, gender-inclusivity safety,"* and a human rights focus is strong.⁵¹

CONCLUSION AND SUGGESTIONS

The deepfake sexual violence is key technological advancement representing violence against women, girls, in the most extreme form. The unfair use of AI for producing pornographic images without consent is direct infringement of *"Article 21 of the Indian Constitution which guarantees the right of privacy, dignity, autonomy, and equality."* The IT Act and DPDP 2023 are two existing legal framework that offer some redress but are still disconnected and hopelessly insufficient when it comes to the *"extent, rate, and anonymity of the illicit use of deepfake technology."* UNESCO's AI governance, the ethical recommendations point out that in terms of Indian AI governance, the ethical values of *"consent, accountability, transparency, and do not harm"* are not only partially but also very poorly executed. Deepfakes go ahead

⁵⁰ Wachter S and Mittelstadt B, *"A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI"* (Center for Open Science 2018) <https://doi.org/10.31228/osf.io/mu2kf> accessed January 4, 2026

⁵¹ Chesney R and Citron D, *"Deepfakes and the New Disinformation War"* (Foreign Affairs, December 11, 2018) <https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war> accessed January 4, 2026

than just hurting the particular victims; they also have negative “*impacts on the trust of the people in general,*” on the exercise of one’s right to express oneself, on the involvement of the public in online democratic processes. If there are no particular rules for controlling the use of deepfake technology, the technology may strengthen the “*present patriarchal power structure*” that are dominated by men and make the conditions of women in society worse, in terms of discrimination, on a large scale.

- Enact special legislation on Deepfake creation and dissemination with increased penalties for non-consensual sexual images.
- Create specific and clear statutory obligations on intermediaries and platforms for quick, detection, takedown, and report deepfake sexual content with tough deadline supporting and responsibility.
- The DPDP Act and rules would be strengthened by overcoming the problems of identifying the deepfakes as personal data abuse and introducing a strong right to erasure and retrieval.
- Demand algorithms transparency and responsibility audits for AI system capable of production of Artificial Media
- Bestows victim-centric measures, like speedy legal proceedings, psychological assistant, and reputation-restoration processes.