SUPREMO AMICUS

VOLUME 40 | February, 2026 ISSN 2456-9704

DEEPFAKES CONSENT AND THE LAW: A FEMINIST CRITIQUE OF DIGITAL SEXUAL VIOLENCE

***By** Shreya Sriram*
***From** Symbiosis Law School, Pune*

I. Introduction

Deepfakes[1] are an advanced artificial intelligence (AI) technology that uses deep learning algorithms to place one face over another, producing extremely realistic fake images or videos. The algorithm does this by analysing one's facial structure from gathered data, studying their angles and expressions, and then reproducing them on the face of another individual to copy their expressions. More generally, deepfakes are a form of synthetic media, including images, videos, or audio edited or produced by AI, AI-powered tools, or audio-visual[2] (AV) editing software. They especially utilise machine learning and AI methods, like facial recognition software and artificial neural networks like variational autoencoders (VAEs) and generative adversarial networks (GANs). In contrast to conventional fake material, deepfakes' utilisation of such sophisticated processes makes them especially powerful.

The popularity of deepfakes is due to several key reasons. Deepfakes started gaining extensive attention from the public in 2018[3] and can be produced with publicly available videos or images. The technology has become easily accessible, with user-friendly, open-source software and applications such as DeepFaceLab, Faceswap, ReFace, and Zao, bringing their production into the reach of people without specialised knowledge. High-performance computing offers the immense processing capacity needed, and video editing applications increasingly employ AI technologies to maximise realism. The pornography market has been a leading force, with 96% of deepfakes consisting of non-consensual pornography, with the internet's heightened accessibility, anonymity, and affordability creating a situation in which deepfakes flourish under the false pretence of authenticity and continue to exist because of the extensive market for this content. One major challenge to containing their spread is the expeditious progress of deepfake creation technology that constantly outpaces the evolution of AI detection software, rendering it ever more challenging to detect and eliminate synthetic content.

This tech is becoming widely recognised as a feminist legal problem[4] because it's disproportionately affecting women and overlapping with existing gender inequality and image-based sexual abuse. Deepfakes, and specifically non-consensual deepfake pornography, are a type of technology-facilitated sexual violence (TFSV)[5]. Women and, more shockingly, minors are disproportionately the victims

[1] Chidera Okolie, 'Artificial Intelligence-Altered Videos (Deepfakes), Image-Based Artificial Intelligence-Altered Videos (Deepfakes), Image-Based Sexual Abuse, and Data Privacy Concerns Sexual Abuse, and Data Privacy Concerns' (2023) 25 Journal of International women's studies <https://vc.bridgew.edu/jiws/vol25/iss2/11?utm_source=vc.bridgew.edu%2Fjiws%2Fvol25%2Fiss2%2F11&utm_medium=PDF&utm_campaign=PDFCoverPages>.

[2] Kinza Yasar, Nick Barney and Ivy Wigmore, 'What Is Deepfake Technology?' (*Tech Target*, 22 May 2025) <https://www.techtarget.com/whatis/definition/deepfake>.

[3] 'Increasing Threat of DeepFake Identities' <https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf>.

[4] Beatriz Kira, 'Deepfakes, the Weaponisation of AI Against Women and Possible Solution' (*Verfassung*, 3 June 2024) <https://verfassungsblog.de/deepfakes-ncid-ai-regulation/>.

[5] Georgia Wood, 'Disinformation and Deepfakes: Countering Gender-Based Online Harassment' (*Center for strategic and International studies*) <https://www.csis.org/events/disinformation-and-deepfakes-countering-gender-based-online-harassment>.

of such content, which results in significant reputational damage, social stigmatisation, and adverse societal attitudes that accentuate underlying gender inequality and the sexualisation and commodification of women. The production and distribution of deepfakes[6], particularly pornographic deepfakes, are morally concerning because they take advantage of existing gender inequality, compounding women's inability to control their bodies and images, as well as perpetuating damaging societal norms. Philosophers go so far as to position deepfakes as an "epistemic threat" to knowledge and society, and studies have reported that women, LGBT individuals, and people of colour are more likely to be targeted[7]. Of particular concern is the absence of sufficient legal frameworks that are specifically put in place to govern deepfake pornography. Such a lack is a reflection of an implicit failure by society to fully address the novel digital harms faced overwhelmingly by women and how patriarchal presumptions regarding autonomy and harm might be embedded in or constitute the prevailing legal methods. Although deepfakes in themselves are legal unless they run counter to current legislation, such as child pornography, defamation, or hate speech, the public's lack of knowledge of the risks posed by the technology is a partial reason why there is no special legislation. The poor legal response to deepfakes makes it challenging to combat the gendered inequality caused by deepfakes and offer adequate means of justice and redress for victims. In addition, deepfakes essentially disempower digital consent and personal agency by producing intimate material without the person in question knowing or consenting to such. This relates directly to broader feminist legal issues around bodily autonomy and consent, primarily when images of women are used, and how this may not necessarily be understood by existing legal frameworks as thoroughly comprehending the systemic breaches of consent involved in non-consensual deepfake production and sharing.

Therefore, this paper will explore how adequately current Indian laws address deepfake-based sexual violence and how a feminist legal lens might expose and remedy these shortcomings. This will involve an analysis of existing legal frameworks and their applicability, or lack thereof, to the specific harms of deepfakes, framed through a lens that prioritises gender equality and the protection of digital autonomy.

ii. Methodology

The study employs a qualitative, doctrinal, and feminist legal approach to scrutinise the legal and socio-cultural implications of deepfake pornography in India and relate to global legal trends. The study explores how current legal paradigms in India conceptualise and address non-consensual synthetic media and whether these paradigms adequately capture the harm inflicted through deepfake technology. The qualitative nature of this study enables a subtle, interpretive examination of laws, judgments, legal texts, scholarly literature, policy reports, and media reports on deepfakes and image-based sexual abuse.

Doctrinal legal research examines pertinent statutory provisions, such as the Indian Penal Code, 1860[8] and the Information Technology Act, 2000[9], and how they apply to deepfake-based harms. International comparative approaches are researched from jurisdictions like the United Kingdom, the United States, and South Korea, which have legislated specific laws or policies tackling deepfake content and digital sexual violence. The comparisons provide insight into reform's potentialities and constraining limits in the Indian setting.

[6] International LLP Hogan Lovells, ‘BRIEFING PAPER: DEEPFAKE IMAGE-BASED SEXUAL ABUSE, TECH-FACILITATED SEXUAL EXPLOITATION AND THE LAW’ <https://equalitynow.org/resource/briefing-paper-deepfake-image-based-sexual-abuse-tech-facilitated-sexual-exploitation-and-the-law/>.

[7] Okolie (n 1).

[8] Indian penal code 1862.

[9] Information Technology Act, 2000.

Embedded in this research is a feminist legal critique, which questions the extent to which current laws embody patriarchal norms around harm, consent, and autonomy. The paper engages with feminist jurisprudence and scholarship to examine how legal traditions have traditionally excluded women's experiences—most notably sexual and reputational harm—and how these tendencies are replicated in the digital sphere through the law's lack of adequate attention to non-physical, technology-enabled harms. Terms like technology-facilitated sexual violence (TFSV), informational consent, and digital embodiment are invoked to situate the discussion and challenge the gender-blindness of conventional legal frameworks.

This approach not only allows for thorough legal examination but also addresses gender justice and critical analysis of systems, and thus is ideally suited to assess how Indian law should develop to address the threats of deepfake technology on a feminist and rights-oriented basis.

iii. Findings

A. The weaponisation of deepfake technology

Deepfakes are a revolutionary and, in some respects, threatening use of artificial intelligence (AI). Constructed on sophisticated deep learning algorithms, they enable the unobtrusive overlay of one individual's face or voice onto someone else's body or speech, producing hyper-realistic but fabricated media[10]. The reason deepfakes are particularly concerning is the enhanced production facility. A recent reporter's inquiry illustrated that an individual might be non-consensually inserted into adult content for as little as $30 with only a 15-second Instagram story and minimal software[11]. As the process is only a few minutes long and requires no technical proficiency, one does not have to be a coder or developer to participate in this abuse. This democratisation of high-end AI technology moved deepfake production from specialist cybercrime to an ordinary potential weapon of harassment, which multiple individuals across the globe are heavily misusing.

The most pervasive and alarming use of deepfake technology, in addition to fraud, has been the production of non-consensual sexually explicit material, disproportionately affecting women and girls. This abuse form is not speculative or future fantasy; it is prevalent, real, and expanding.

A 2023 McAfee survey found that over 75% of Indian internet users[12] had viewed a deepfake in the past year. Sensity AI, a deepfake detection firm, says 90–95% of deepfake content worldwide is pornography, and 99% of victims are women. By October 2020, more than 100,000 fake nude photos of women were created and shared without their consent, mostly on encrypted messaging apps like Telegram. Shockingly, many victims were minors.

In a global survey of 10 nations[13], 2.2% of participants said they were personally victimised by deepfake pornography, and 1.8% confessed to being perpetrators. Consumption of celebrity deepfake porn was reported by 6.2%, demonstrating a troubling normalisation of such material. Men are statistically more likely to report having looked at, made, or shared deepfake porn. Yet, women overwhelmingly suffer the consequences of being featured in it, although the men admitted to having consensually watched or

[10] 'The Tensions of Deepfakes.'

[11] Vittoria Elliott, 'Celebrity Deepfake Porn Cases Will Be Investigated by Meta Oversight Board' [2024] *WIRED* <https://www.wired.com/story/meta-oversight-board-deepfake-porn-facebook-instagram/?utm_source=chatgpt.com>.

[12] '75% Indians Have Viewed Some Deepfake Content in Last 12 Months, Says McAfee Survey' *The economic Times* (25 April 2024).

[13] Rebecca Umbach and others, 'Non-Consensual Synthetic Intimate Imagery: Prevalence, Attitudes, and Knowledge in 10 Countries', *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (2024).

shared this deepfake content. Still, women have been featured non-consensually in it. This gender imbalance points to a consumption/target dynamic in which women's bodies are seized and commodified by new technologies without their consent.

India's public confrontation with deepfakes intensified when a sexually provocative AI-made clip of actress Rashmika Mandanna[14] went viral. Although false, the video was credible enough to deceive many people. Prime Minister Narendra Modi spoke out publicly, and tech companies were called upon to act, which was a considerable effort against the propagation of deepfake technology; however, the enforcement of the rules has, till now, been quite inconsistent.

Globally, the incident of Noelle Martin[15], an Australian law student, has become symbolic. Martin's pictures, which were taken when she was 17 years old, were edited into pornography content that later emerged in the form of deepfake videos for years. They were sent to her via email and posted on various pornography websites, leaving no possibility of deletion or tracing their origin. Her reputation, psychiatric well-being, and career opportunities were negatively affected despite legal action. Her account highlights how deepfake abuse[16] aggravates the harms of regular image-based sexual abuse, perpetuating trauma across time and space and producing a digital trace that is almost impossible to delete.

Brooke Monk[17], a prominent American digital content creator with over 32 million followers on TikTok and a significant presence across YouTube and other platforms, who initially gained her popularity through lifestyle, fashion, lip-sync, and dance videos, was pushed into the limelight for the wrong reasons, when a nude original video reportedly featuring her was leaked, sparking widespread discussion about online safety, privacy, and digital culture. This incident was worsened by a misleading video claiming to show explicit images of her, released by another user known as "K." This video rapidly spread false content, severely compromising her privacy and mental well-being. It was later discovered that a deepfake image of Monk shared on Twitter was digitally altered and not genuine, highlighting the issue of deepfake misuse in her case.

The viral spread of this content underscored how easily personal boundaries can be breached in the age of social media, driven by a mix of curiosity, outrage, and the human tendency to spread gossip, leading to a profound loss of control over her narrative. Brooke Monk publicly expressed her anguish and frustration through social media, exposing the hurtful consequences of being dehumanised and humiliated by these actions, further showcasing the impact of such harmful use of deepfake technology. She released a video about the situation. She denied any involvement in explicit content and stressed the importance of responsible online behaviour. She urged her followers to report such incidents instead of sharing them. Her supporters rallied around her, defending her and expressing outrage over the fake images, thus fuelling the discussion for misuse of artificial intelligence and the lack of boundaries when it comes to the creation of such degrading content.

The Brooke Monk incident has illuminated several critical issues within the digital realm. It serves as a stark reminder of the pressing need for stronger measures to protect individuals' private information, especially for online influencers who face inherent risks due to their public presence. The rapid dissemination of private moments highlights the

[14] Abhinaba Datta and Subarno Banerjee, 'Unmasking Deepfakes-A Legal Perspective' (2023) 4 Jus Corpus LJ 336.

[15] Noelle Martin, 'Image-Based Sexual Abuse and Deepfakes: A Survivor Turned Activist's Perspective' [2021] The Palgrave Handbook of Gendered Violence and Technology 55.

[16] Benjamin T Suslavich, 'Nonconsensual Deepfakes: A" Deep Problem" for Victims' (2023) 33 Alb. LJ Sci. & Tech. 160.

[17] Lina Schaden V, 'Brooke Monk Leaks: Unpacking The Viral Rumors And Digital Footprint' (*Procamp*) <https://www.procamp.qa/tiktoknews-007/brooke-monk-nude-leaks/>.

"darker side[18]" of social media saturation; despite the fame and glory that comes with it, the risk of such videos being made, with initial platform responses often being slow, allowing content to spread widely before removal. From a legal standpoint, disseminating private content without consent raises significant concerns, as such actions can violate privacy laws in many jurisdictions. Ethically, sharing someone's private content without permission is a serious breach, emphasising the need for a more responsible approach to handling sensitive information and respecting individual privacy.

And, just like Brooke Monk, international stars such as Kristen Bell, Scarlett Johansson and Gal Gadot have all been subjected to deepfake pornography. Even prominent public figures with access to excellent legal and financial resources are powerless to stop this abuse, which indicates how helpless the average victim might feel.

B. Deepfakes as Technology-Facilitated Sexual Violence (TFSV)

Deepfake pornography from a feminist legal framework is technology-facilitated sexual violence (TFSV), a digital offshoot of patriarchal violence. While no physical contact is involved, no physical interaction is required, and the harm caused is real and lasting. The non-consensual character of deepfake porn is identical to that of sexual assault: it is a violation of bodily and sexual autonomy, created digitally but socially and psychologically harmful.

At the core of feminist legal theory is the premise that consent[19] is communicative and contextual. Deepfake pornography[20] annihilates this paradigm. It entails no consent whatsoever at any point, not when the image is used, not when it is manipulated digitally, and not when it is shared. Victims themselves might not even know their image has been used until others have already viewed or forwarded it or popularised it in the media. This detachment of the body from agency parallels the commodification of women's bodies in other legal and cultural spheres but with more sinister implications because it is disguised as "virtual."

Victims experience psychological reactions similar to PTSD: re-traumatisation, loss of identity, fear of being seen, and even false memories, as their authentic selves become intertwined with fictional representations. The idea of "digital infinity," the internet's ability to save and reproduce content infinitely, is that the damage is endless. One deepfake can be downloaded, shared, mirrored, and re-uploaded on dozens of sites in hours, with no definite possibility or scope to be taken down.

The moral construction of deepfakes remains in the process of developing, yet contemporary social opinion is saturated in misunderstanding and minimisation. Empirical research indicates that men are most likely to consume deepfake pornography[21][22] and least likely to view it as "dangerous." Others even consider it an entertainment or "fantasy." This highlights how structural gender inequality operates in informing both the reception and production of deepfake material.

[18] Djamila Kadem and Kafia Mohamed Eltaib Lassouane, 'The Negative Impact of Deepfake Technology on the Reputation of Prominent Figures on Social Media Platforms: An Analytical Study on a Sample of Fabricated Videos.' (2024) 4 Journal of Science and Knowledge Horizons 510.

[19] Anastasia Karagianni and Miriam Doh and, 'A Feminist Legal Analysis of Non-Consensual Sexualized Deepfakes: Contextualizing Its Impact as AI-Generated Image-Based Violence under EU Law' (2024) 0 Porn Studies 1.

[20] Carl Öhman, 'Introducing the Pervert's Dilemma: A Contribution to the Critique of Deepfake Pornography' (2020) 22 Ethics and Information Technology 133.

[21] Prachi H Bhuptani and others, 'Pornography Use, Perceived Peer Norms, and Attitudes Toward Women: A Study of College Men.' (2024) 19 American journal of sexuality education 280.

[22] Umbach and others (n 13).

In interviews[23], some of the participants thought that destigmatising sex and pornography might diminish the harm of deepfakes[24], but only at the expense of holding victims responsible for not being as affected, not perpetrators for ceasing. Others rationalised their interest in deepfakes by referencing memes or fanfiction[25], similarly within appropriateness, disregarding the intent to deceive and violate consent that distinguishes deepfakes from satire, taking a more comical approach than a serious solution. Critically, society has not yet recognised deepfake pornography as sexual violence[26], even though its psychological and reputational damage is evident. This is especially so in legal frameworks that still give precedence to corporeal harm over emotional, social, or reputational harm, depriving digital victims of sexual violence of their rights, which are being violated.

Although some countries have started drafting laws for redressing deepfake harms, most nations, including India, have no such statutes criminalising deepfake pornography. Indian law presently deals with image-based sexual abuse under the Information Technology Act, 2000 and the Indian Penal Code, 1860, but such provisions prove inadequate when dealing with AI-produced content.:

This legal uncertainty leaves loopholes through which abusers can function scot-free. Deepfake artists tend to be located outside the country, so it becomes an even more challenging task to enforce across borders. The insufficient deterrence and limited avenues to justice add to the helplessness that victims complain about.

As much as legal remedies are non-existent, the technology used to make deepfakes is improving at a frightening rate. More advanced tools can now produce audio deepfakes, live-streamed impersonation, and real-time face swapping[27], making it increasingly challenging to detect the already-hard-to-spot deceptions. Although AI-based detection tools exist[28], they are not yet public-facing, unreliable, and need large computational capacities. Moreover, deepfake technology itself advances so fast that it bypasses detection tools as a whole, and if it does, platforms have been accused of not effectively using these tools.

The lag between harm and remedy, both technically and legally, is that victims suffer long before the state or platforms can intervene. This enforcement lag is not only a policy failure but gendered harm, as it stems from a deeper systemic failure to consider women's digital safety seriously.

C. Overview of Indian laws on deepfake technology

While India does not yet possess a specific law[29] solely targeting deepfake technology, the existing legal framework, anchored in the Indian Penal Code (IPC) and the Information Technology (IT) Act of 2000, is being cautiously extended to address its harmful manifestations. However, this patchwork approach reveals deep and troubling gaps in both

[23] Natalie Grace Brigham and others, '" Violation of My {body:}" Perceptions of {AI-Generated} Non-Consensual (Intimate) Imagery', *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)* (2024).

[25] Jacquelyn Burkell and Chandell Gosse, 'Nothing New Here: Emphasizing the Social and Cultural Context of Deepfakes' [2019] First Monday.

[26] Carl Öhman, 'Introducing the Pervert's Dilemma: A Contribution to the Critique of Deepfake Pornography' (2020) 22 Ethics and Information Technology 133.

[27] Jules Roscoe, 'Deepfake Scams Are Distorting Reality Itself' [2025] *WIRED* <https://www.wired.com/story/youre-not-ready-for-ai-powered-scams/>.

[28] Simiao Ren and others, 'Do Deepfake Detectors Work in Reality?' [2025] arXiv preprint arXiv:2502.10920.

[29] Vasundhara Shankar, 'Deepfakes Call for Stronger Laws' *The Hindu Business Line* (16 July 2023) <https://www.thehindubusinessline.com/business-laws/deepfakes-call-for-stronger-laws/article67077019.ece>.

scope and effectiveness, particularly in addressing the nuanced harms inflicted by deepfake pornography and other non-consensual AI-generated content. Existing legislation is backwards-looking as opposed to forward-thinking and not well adapted to meet the unique challenge of deepfakes, media that is not just false or obscene but artificially created to mislead and shame, frequently with long-term psychological, reputational, and social impacts on the victim.

The majority of such provisions do not criminalise deepfakes per se but rather criminalise the larger consequences they can cause, i.e., defamation (Sections 499–500 IPC), cyber cheating and impersonation (Sections 66C–66D IT Act), or dissemination of obscene material (Sections 67, 67A IT Act). These provisions call for the imposition of established categories over new digital harms, producing interpretive uncertainty and leaving no statutory guidance for enforcement agencies about how to prosecute synthetic sexual violence. For example, obscenity laws will be engaged by deepfake pornography, but they tend to require a threshold of public harm or indecency to be exceeded. Suppose a deepfake is in private circulation or does not show explicit nudity. In that case, it may not cross these legal thresholds but still grossly violate the person's dignity, privacy, and consent. This fails to meet the law's sensitivity to deepfakes' particular intentionality and impact, where even suggestive tampering can ruin a person's personal and professional life.

Compounding the issue further is that these statutes were not envisioned in a technological framework in which image manipulation was possible without explicit access to the victim. Conventional voyeurism or non-consensual image-based sexual abuse statutes (e.g., Section 354C[30] IPC) are based on the notion that the original content or the interaction existed. But deepfakes destroy this presumption; they enable perpetrators to produce sexualised depictions of people, including children, never having physically seen them, let alone recorded explicit material. This destabilises traditional evidentiary models of Indian law (like assault[31]), which tend to rely on establishing actual contact or recording. Without statutory protection of "synthetic" sexual images, the victims fall into a legal void in which they cannot precisely assert their right to privacy or bodily autonomy since the photos, technically, are "not real."

Also, the Indian judicial process continues to be slow and cumbersome, especially in cyber abuse cases. They are frequently confronted with a Kafkaesque labyrinth of legal procedures, minimal institutional or police assistance, and few streamlined mechanisms to have content removed promptly[32][33]. Police forces lack the training and technical ability to investigate cybercrimes such as deepfakes, particularly when the attackers are anonymous or from overseas. Overlaid on top of this is the splintered jurisdiction over internet sites, some of which are based in foreign nations and beyond Indian legal reach without extensive international cooperation. The result is a legal culture in which justice isn't just delayed but frequently denied altogether. Before one can even file an FIR, the material might have already been reposted thousands of times, saved by random strangers, reposted, and etched into the electronic ether.

This failure of meaningful legal redress and pressure has, in turn, led the government of India to make initial steps toward reform. In November 2023, the Union Government gave an advisory to social media intermediaries, inviting them to remove deepfake content within 36 hours of receiving a complaint or

[30] Indian Penal Code 1860, s 354C
[31] Indian Penal Code 1862.
[32] Karan Choudhary and Mahak Rajpal, 'CRIMINALIZING DEEPFAKE TECHNOLOGY IN INDIA: A LEGAL ANALYSIS OF PRIVACY AND REGULATORY GAPS' [2025] INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH.
[33] Sayobani Basu Basu and Durga Priya Manda, 'Generative Artificial Intelligence – India's Attempt at Controlling "Deepfakes"' (*Chambers and Partners*) <https://chambers.com/legal-trends/controlling-deepfakes-in-india>.

risk having their safe harbour immunity under the IT Act withdrawn[34]. This was an important step, but it still keeps the responsibility of identification and complaint on the victim and does not institutionalise proactive detection or platform-level accountability yet. Concurrently, these efforts are still policy-level actions instead of codified legal requirements, i.e., they are not enforceable until translated into legislation or formal rulemaking.

Encouragingly, the courts have started to acknowledge the imperative of safeguarding individuals' digital identity and personality rights in an era of AI. In trailblazer cases, stars such as Amitabh Bachchan[35] and Anil Kapoor[36] were awarded injunctions against the unauthorised use of their name, likeness, and image by means of deepfake technology. The cases are notable not because they provide statutory remedies for all victims but because they symbolically affirm the right to defend one's "persona" as a recognised interest in law against deepfake abuse. However, this remedy is still only available in large part to those with the resources and visibility to bring cases, leaving many ordinary victims, particularly women and vulnerable groups, without effective recourse or public scrutiny.

The imperative of a dedicated, future-proof legal framework is thus pressing. A strong law should acknowledge that deepfake abuse is not just an intensification or expansion of the current offences but a qualitatively different kind of digital harm, one that invades autonomy, consent, and dignity in novel ways. Such a law should criminalise and define the creation and sharing of deepfakes without permission, offer effective content removal mechanisms, require content detection at the platform level and user awareness, and prioritise the experience of the victim and not require them to fulfil archaic legal standards. It should also consider the gendered character of the damage since virtually all victims of deepfake porn are women and use a survivor-centred approach in its redressal mechanisms.

If not for this, India runs the risk of emulating the world trend of legal systems being behind technological abuse and of the social price of innovation being paid disproportionately by women, minorities, and vulnerable groups. In order to successfully counter these, the Indian legal system needs to get beyond outmoded categories and towards a rights-oriented, tech-literate, and gender-sensitive response.

D. Comparison with the legislation of other countries

1. South Korea

South Korea's legal reaction to deepfake pornography and online sexual violence has been both quick and extensive, especially after the public outcry in response to the "Nth Room[37][38]" case back in 2020. This case of massive exploitation and blackmailing of women and minors using sexually exploitative videos on messaging apps like Telegram became a national wake-up call on the insufficiency of digital legislation. The scope of the abuse, compounded by the anonymity of cryptocurrency and overseas-based servers, exposed serious loopholes in the Korean judicial system and further fuelled calls for responsibility and institutional reform. The public outcry following this case led to the government of

[34] Srishti Jha, '"Remove Misinformation, Deepfakes within 36 Hrs": Centre to Social Media Firms' *India Today* (7 November 2023) <https://www.indiatoday.in/india/story/remove-misinformation-deepfakes-within-36-hrs-centre-to-social-media-firms-2460129-2023-11-07>.

[35] Amitabh Bachchan v. Rajat Nagi, (2022) 6 HCC (Del) 641

[36] Anil Kapoor v. Simply Life India, 2023 SCC OnLine Del 6914

[37] Nicole De Souza, 'The Nth Room Case and Modern Slavery in the Digital Space' *The interpreter* (Lowy Institute, 20 April 2020) <https://www.lowyinstitute.org/the-interpreter/nth-room-case-modern-slavery-digital-space>.

[38] Min-sik Yoon, '"Anti-Nth Room" Legislation, an Unfulfilled Promise' *The Korea Herald* (11 July 2022) <https://www.koreaherald.com/article/2909004>.

South Korea implementing an aggressive array of legislative changes, popularly known as the "anti-Nth Room[39]" laws, that not only widened the criminal liabilities for cybersex crimes but also paved the way for how deepfake pornography was to be approached in legislation.

One of the most significant features of the new legislation is broadening criminal liability not only to those making or distributing deepfake pornography[40] but also to those who store, have, or even merely look at such material. This is a remarkable departure from previous legal practice that tended to address only producers or distributors and left the role of passive viewing in facilitating the market for such content untouched. Under the amended law enacted on 26 September 2024, watching sexually exploitative deepfakes for themselves, regardless of whether they have paid for them or downloaded them, is now punishable by up to three years imprisonment or a heavy fine. This is an unmistakable legal acknowledgement that deepfakes are not only digital artefacts but instruments of harm and that their consumers are also, in part, responsible for the violation of the victim's bodily autonomy and digital dignity. The maximum penalty for producing and sharing such content has also been increased to seven years, with intent no longer being a requirement for punishment. This fills a vital gap in which offenders in the past invoked a lack of malice or artistic merit as a defence.

In addition to these new sanctions, current legislation was deeply reformed to meet the changing face of sexual abuse online. The Sexual Violence Punishment Act was rewritten to criminalise not only illicit filming or dissemination but also coercive actions such as threatening someone with the dissemination of sexually exploitative content. Notably, the amendments made clear that consent during filming does not equate to consent for distribution, moving the legal emphasis from the act of creation to the act of dissemination, one of the most urgent legal blind spots for courts in jurisdictions confronting AI-created content. In addition, criminal laws were amended to demonstrate the gravity of such offences by bringing the sentencing for internet sexual offences in line with that for special rape and robbery. These developments signal a parliamentarian grasp that sexual abuse in person or via the web exacts similar psychological and reputation-related wounds on victims.

Another essential support structure of the reform package was the levying of duties on online platforms, search engines, and cloud service providers to monitor their content and act quickly to delete illicit material. The amended Telecommunications Business Act[41] gave these platforms the power to scan group chats, screen uploaded media for obnoxious content, and assist law enforcement, one of the first times that legally binding content moderation requirements were imposed. This expansion of liability to tech intermediaries such as South Korean firms like Kakao and Naver, as well as multinationals like Meta and Google, was a regulatory paradigm shift. Yet even in taking these steps, the reforms also recognised their limitations, especially in platforms headquartered beyond South Korea's jurisdiction. The situation of imitation operations like the "cat Nth room" on foreign encrypted messaging apps highlighted the difficulties of enforcement in a digitally networked globalised space, where laws tend to end at national borders.

Still, despite the above, the reforms have been widely criticised. The most often cited shortcoming is the lack of an independent law specifically targeting the distinct features of deepfake technology. Whereas deepfake pornography is criminalised under wider offences such as illegal production or distribution of obscene content, the legislation does not yet codify or

[39] Stephanie Seng, *Rape Culture in Media Coverage: An Analysis of the" Nth Room" Scandal* (2024).

[40] Reuters, 'South Korea to Criminalize Watching or Possessing Sexually Explicit Deepfakes' *CNN* (26 September 2024) <https://edition.cnn.com/2024/09/26/asia/south-korea-deepfake-bill-passed-intl-hnk>.

[41] Telecommunications Business Act (South Korea), Act No 3920 of 1996, as amended by Act No 17078 of 2019

recognise AI-generated content as a distinct legal concept. Consequently, applying these provisions to synthetic or manipulated material sometimes necessitates interpretive looseness on the part of courts. Prevention is especially under-addressed. Existing laws continue to emphasise post-facto punishment without adequate use of anticipatory regulation or technological infrastructure to detect and ban such content prior to its posting or virality. This has resulted in enforcement lag; most posts flagged for removal have stayed online for days or weeks while the harm has already been done.

South Korea's reforms have also triggered controversies regarding constitutional freedoms. Critics say that making platforms legally responsible and technologically capable[42] of monitoring user content in real-time, even with AI filters, creates serious issues around privacy and overreach. Examples of automated moderation blocking non-obscene content, like beach pics, highlight the shortcomings of existing AI filters and the potential for violating free speech and artistic expression. Simultaneously, law enforcement's heavy reliance on online monitoring and undercover investigations to prosecute sex trafficking rings has raised alarm among privacy activists who are worried about government intrusion into citizens' communications.

Another enforcement challenge stems from prosecution difficulty, particularly with the anonymous, frequently encrypted platforms used to distribute deepfake content. Even with such broad legal reforms, most perpetrators go unidentified, especially when they move across borders or leverage anonymising technologies. In these instances, prosecution grinds to a halt or is rejected, eroding victim confidence in the justice system. Legal specialists have also referred to the absence of investigator emergency search and seizure powers as a key obstacle in pointing to the necessity for instant deletion rights and swift freezing of content and accounts upon finding exploitative content.

Although criticised, South Korea's legislative strategy is among the most aggressive and progressive in the world. It aligns with a universal consensus that online sexual violence, such as deepfakes, should be judged similarly to offline sexual assaults. The reforms are far from perfect, but they present an interesting precedent for jurisdictions such as India that continue to grapple with adapting deepfake harms into lagging law provisions. As the government of Korea works to refine and broaden its legislation in this regard, it provides a shining example of how survivor testimony, public pressure, and legal creativity can come together to effectively address new expressions of gendered violence in the internet age.

2. United States of America

In the U.S[43]., the policy and legal response to deepfakes is patchwork, developing through a series of state statutes, new federal legislation in its final stages of development, and a reliance on existing jurisprudence. These efforts are being designed concurrently with significant industry-initiated efforts. In contrast to nations like South Korea, where legislative change has been more centralised and comprehensive, the U.S. strategy reflects its federal nature and constitutional intricacies surrounding freedom of speech. Although there has been progress, the U.S. response is bound by legal doctrines prioritising the First Amendment and thereby presenting a complex context for regulating dangerous deepfakes, especially where it overlaps with subjects like satire, journalism, and political speech.
In the United States, various jurisdictions have moved proactively to regulate the wrongful use of deepfakes.

[42] Brandon Dang, Martin J Riedl and Matthew Lease, ‘But Who Protects the Moderators? The Case of Crowdsourced Image Moderation’ [2018] arXiv preprint arXiv:1804.10999.

[43] Scott Nover, ‘South Korea Banned Deepfakes. Is That a Realistic Solution for the US?’ *GZero* (8 October 2024) <https://www.gzeromedia.com/gzero-ai/south-korea-banned-deepfakes-is-that-a-realistic-solution-for-the-us>.

California[44], for example, has become the first state to prohibit the creation and distribution of "materially deceptive" deepfakes in political campaign advertising within a specified time frame ahead of elections. The bill makes provision for exemptions involving satire and parody, as long as there is adequate indication that the content is manipulated. Furthermore, California has identified the reputational and emotional damage of sexually explicit deepfakes by providing people with a right to civil redress in case their image is utilised in unwanted pornographic content.[45] Other states, however, have enacted more specifically crafted legislation. For instance, Virginia[46] criminalised the dissemination of sexually explicit pictures that have been computer-altered to convey a particular person's image, focusing on harmful intent. Likewise, Texas and Maryland have addressed electoral integrity by passing or introducing bills criminalising the deployment of deepfakes in elections. These state enactments, while laudable, are highly divergent in intent and breadth, providing unequal protection based on where a person is located. The relative lack of uniformity between states highlights the necessity for a blanket federal law that can set a nationwide standard.

On the federal level, the most profound legislative action was the approval of the "Take It Down" Act[47] on 19 May 2025. This act represents a turning point in the federal government's response to the regulation of non-consensual intimate imagery, such as deepfake pornography. According to the Act, it is a federal offence to knowingly post sexually explicit material, actual or digitally manipulated, without the express permission of the person involved. This is also the case with authentic and synthetic, AI-generated depictions, which are defined, albeit separately, under the act. The law makes distinctions between content involving adults and minors, where greater punishment has been meted out for the latter, including imprisonment for a term of up to three years. Significantly, the act also provides for a notification mechanism by victims to hosting platforms for the removal of offending content. Covered platforms, such as websites and applications that host user-created content, are required by law to have systems in place for receiving and responding to such takedown requests. This has significant implications for schools, which will need to update conduct policies and get ready to comply with subpoenas and administrative protocols for online sexual misconduct with students or employees.

Despite the progress represented by the Take It Down Act, federal legislative initiatives remain limited in breadth and enforcement clarity. Several bills have been introduced to improve understanding of the technology behind deepfakes and their national security implications. For example, the Identifying Outputs of Generative Adversarial Networks (IOGAN) Act suggests that the National Science Foundation and National Institute of Standards and Technology fund research into software utilised in creating deepfakes. Similarly, the proposed legislation would mandate that federal agencies like Homeland Security and Defence explore how deepfake technologies affect military members and national infrastructure. Although these efforts seek to establish institutional consciousness and technological readiness, they do not go as far as delivering full-

[44] Rob Garver, 'California Laws Target Deepfake Political Ads, Disinformation' [2024] *Voa News* <https://www.voanews.com/a/california-laws-target-deepfake-political-ads-disinformation/7789746.html>.

[45] TRÂN NGUYỄN, 'California Governor Signs Bills to Protect Children from AI Deepfake Nudes' *AP News* (30 September 2024) <https://apnews.com/article/ai-deepfakes-children-abuse-7dcf5c566e2a297567f1e148ac2074a4>.

[46] Adi Robertson, 'Virginia's "Revenge Porn" Laws Now Officially Cover Deepfakes' *The Verge* (2 July 2019) <https://www.theverge.com/2019/7/1/20677800/virginia-revenge-porn-deepfakes-nonconsensual-photos-videos-ban-goes-into-effect>.

[47] Tiffany Hsu, 'Deepfake Laws Bring Prosecution and Penalties, but Also Pushback' *NY Times* (22 May 2025) <https://www.nytimes.com/2025/05/22/business/media/deepfakes-laws-free-speech.html>.

fledged legal mechanisms for victim remedy or content moderation.

The most debated[48] recent federal proposal is the DEEPFAKES Accountability Act[49], which requires those who produce synthetic media to add watermarks and acknowledgements clearly indicating the content has been manipulated. The bill also mandates harsh penalties of up to $150,000 per occurrence for not labelling or for stripping away such disclosures. Impacted persons would enjoy a private right of action to sue creators for misuse of their likeness. However, the bill has faced vigorous opposition from civil liberties organisations and legal experts, who claim that the legislation will have a chilling effect on constitutionally protected expressions like parody, political satire, or fiction writing. Because the First Amendment promises strong protections for speech, any regulation of deepfakes will need to be narrowly drawn and prove that it does not violate constitutionally protected expression unless it is pursued with actual malice or creates demonstrable harm.

Another level of complication stems from the weaknesses in current U.S. laws applying to deepfakes. Legal action for victims is currently largely reliant on general tort law, copyright rights and rights of publicity. These legal avenues are typically costly and time-consuming and involve the necessity of knowing the perpetrator, an especially challenging requirement in cases involving anonymised or foreign perpetrators. Although victims can bring actions for defamation or intentional infliction of emotional distress, these are only available actions when the manipulated content is clearly harmful and does not enjoy protection as free speech. Moreover, Section 230 of the Communications Decency Act[50] continues to immunise platforms against liability for user-generated content, severely limiting victims' recourse to force platforms to remove or moderate deepfake content. Consequently, sites such as Facebook, X (previously Twitter), and Reddit cannot, in general, be held responsible for hosting or sharing deepfakes, even when such materials inflict significant reputational harm.

Acknowledging these constraints, various private and governmental players have resorted to technological measures to mitigate the dissemination of deepfakes. Most large platforms have revised their terms of service to prohibit direct deceptive synthetic media. Meanwhile, organisations and researchers have teamed up to create detection tools, such as publicly available databases of known deepfakes for training machine learning algorithms. Programs like the Deepfake Detection Challenge[51], which provided significant cash prizes for successful detection platforms, seek to remain ahead of continually evolving AI tools. The Pentagon's Defence Advanced Research Projects Agency (DARPA) has entered the fray as well, actively creating deepfakes in-house to test and develop identification technologies. This is a manifestation of the increasing acknowledgement that regulation would not be enough; instead, technical innovation will be the key to addressing the harms that synthetic media can cause.

In the future, the prospects of meaningful regulation of deepfakes in the United States are uncertain. As awareness increases and legal and technological frameworks are under development, legal reform is behind the rapid pace at which synthetic content is developing. Cooperation from the industry and

[48] Arthur Holland Michel, 'The ACLU Fights for Your Constitutional Right to Make Deepfakes' *WIRED* (24 July 2024).

[49] Christopher Sundquist, '(Deep)fake News' (5 November 2019) *Science and Technology Law Review* https://journals.library.columbia.edu/index.php/stlr/article/view/6252 accessed 18 June 2025

[50] Communications Decency Act, 47 USC § 230 (1996)

[51] Sam Sabin, 'Deepfakes Are Easy to Make, but Also Easy to Detect' (*Axios*, 12 August 2024) <https://www.axios.com/2024/08/12/def-con-darpa-deepfake-lab?>.

innovation will be essential, particularly since there are restrictions under the U.S. Constitution. However, as new accusations surface and public pressure escalates, there can be an opportunity for further tightening of legislation that maintains a delicate balance between the safeguarding of victims and the freedom of expression.

3. United Kingdom

The United Kingdom has been increasingly building an integrated legal response to address the development of deepfake technology, specifically in relation to its application in the non-consensual production of sexually explicit material. This response has been formulated through newly proposed and enacted legislation criminalising both the production and sharing of explicit artificial media and broadening the protection for individuals, particularly women and girls, who are disproportionately subjected to such abuse. The government's response is not only legislative but also institutional and cultural, seeking to transform the social and technological context that makes deepfake abuse possible.

At the heart of the UK's changing legal landscape is the creation of new criminal offences[52] that target the special harms posed by deepfakes in a direct way. Perhaps the most critical development is the planned offence of making a sexually explicit deepfake image. In contrast to the earlier legal provisions demanding proof of distribution or harm caused to the public, this law criminalises the creation itself if it is undertaken with the aim of causing alarm, humiliation, or distress. This signifies a crucial change towards the acceptance that the psychological and emotional harm resulting from these images, whether or not they are shared, needs to be acknowledged. Where an individual both creates and distributes such a deepfake, they are liable for two distinct offences, permitting the possible imposition of more severe penalties and indicating the gravity of the behaviour.

The legal framework also widens its scope with the criminalisation of capturing or filming intimate photos without consent. Drawing on existing legislation, such as prohibitions of "upskirting," these new crimes widen the coverage of the conduct made criminal. The law will now cover cases where intimate photographs are taken without permission, be it with or without the intention of doing so to cause harm or for sexual gratification. Notably, it also criminalises cases where an individual may say they did not know that consent was needed unless they had a reasonable belief to that end. By creating offences that cater to various motives, whether to humiliate, to gratify sexual desire, or to control, the law aims to account for a variety of abusive behaviours long left unpunished as a result of very narrow or outmoded legal concepts.

In another step to enhance preventative measures, the UK will also criminalise installing or maintaining equipment, in this case, covertly installed cameras or spyware, purposefully to facilitate these image-based abuses. This measure shows a prospective tack by recognising that technology-assisted abuse usually starts much earlier than actual image creation or distribution. It enables the law to act at an earlier point, minimising the chances that such photographs are ever created or distributed.

The new offences are serious in themselves. For instance, creating sexually explicit deepfakes can result in prosecution for a potentially unlimited fine. In combination with the sharing of the content, custodial sentences are likely to be imposed. Those convicted of taking intimate images without consent can face up to two years in prison. The same penalty applies to individuals found guilty of installing equipment with the intent to commit such offences. These penalties not only reflect the gravity of the offences but also serve as a deterrent aimed at both would-be offenders and technology developers who might facilitate such behaviour.

[52] Ministry of Justice and Alex Davies-Jones MP, ‘Government Crackdown on Explicit Deepfakes’.

Notably, the interventions are precisely designed to apply mainly to adult victims, as existing legislation already criminalises comparable behaviour for children's images. This distinction enables the law to fill important gaps in adult protection legislation without duplicating efforts in the realm of child protection. In reality, this means that the adults who were once left with no adequate legal redress for deepfake abuse can now avail themselves of justice via a more victim-focused and responsive justice system.

The new crimes are part of an overall package of legislation within the Criminal Justice Bill, which is being utilised as a vehicle to bring about these changes. It was reported in January 2025[53] that the offences of making sexually explicit deepfakes and intimate image abuse would also be added to the upcoming Crime and Policing Bill, demonstrating the government's intention to mainstream these protections in more than one legal tool. These measures are built on the initial Online Safety Act (2023), which criminalised the sharing of non-consensual deepfake photos and imposed a requirement on platforms to delete toxic content. Sexual Offences Act 2003 was also amended to harden the law even further by adding provisions for criminalising the sharing or the threat of sharing indecent images, including deepfakes, to cause distress. In September 2024[54], online image offences, including intimate photos, were made "priority offences" under the Online Safety Act, and tech platforms have to actively monitor and take down such content or risk being taken enforcement action by Ofcom, the UK communications regulator.

The government's approach to countering deepfake abuse is built into its wider Plan for Change, which focuses on addressing online harms and enhancing the criminal justice response to violence against women and girls. Identifying such violence as a threat to the nation, the UK has tasked police forces with earmarking investigations into image-based abuse as a priority and enhancing their responsiveness to digital harms. These reforms are not merely punitive but are meant to change public attitudes, strengthen social norms against technology abuse, and prevent victims, who are overwhelmingly women, from being silenced or stigmatised for crimes committed against them.

The state's initiative is coupled with an expectation of heightened accountability on the part of the technology industry. The Technology Minister[55], Baroness Jones, has also highlighted that tech businesses need to do more to track content, take down toxic media, and invest in detection software that can identify whether imagery is authentic or manipulated. User-generated content platforms are being subjected to stricter examination, and non-compliance with regulatory requirements could lead to substantial fiscal and legal costs. This is a recognition increasing around the world that private companies need to take an active role in stopping abuse enabled by their platforms and not just respond to it afterwards.

Overall, the United Kingdom's regulation of sexually explicit deepfakes is a forward-thinking and victim-led model that unites new criminal offences with current legal protections. By criminalising the production, distribution, and facilitation of such material and by making both producers and sites liable, the UK is establishing a stronger legal framework in which victims of digital sexual abuse can receive redress and dignity. While there are difficulties still to be overcome, especially in terms of enforcement and technological identification, the legal changes are a strong indication of the

[53] ibid.

[54] Department for Science, Innovation and Technology, and Ministry of Justice, ‘Crackdown on Intimate Image Abuse as Government Strengthens Online Safety Laws’ *Gov.UK* (13 September 2024).

[55] Oscar Hornstein, ‘Tech Minister on Regulating Big Tech and Tackling Online Hate’ (*UK TECH NEWS*, 26 August 2024) <https://www.uktech.news/news/government-and-policy/tech-minister-on-regulating-big-tech-and-tackling-online-hate-20240826?>.

determination to ensure that the law remains ahead of new digital harms.

E. Feminist view

The deepfake porn regulation demonstrates how the law remains based on male-conceived concepts of harm, autonomy, and personhood, a complaint long set out by feminist legal theorists. Androcentric epistemologies[56] have informed traditional legal frameworks to consistently favour harms that are visible, measurable, and economical in kind, closest to masculine-coded experiences. Feminist scholars such as Catharine MacKinnon[57] and Mari Matsuda[58], for instance, contend that the law tends to neglect or downplay harms disproportionately experienced by women, especially those based on sexuality, objectification, and dignity-degrading harms. In deepfakes, this comes in the form of the law's past resistance to see image-based sexual abuse as grave harm, except where it occasions concrete economic loss or even general public devastation. Feminist legal theory requires a more expansive understanding of harm, one that seriously considers the emotional, psychological, and social harms done by being digitally dispossessed of autonomy and agency. Producing a sexually explicit deepfake, no matter if it is never disseminated more broadly, amounts to an insult to the subject's dignity. It makes the female body a virtual site of conquest and consumption, reaffirming patriarchal norms that treat women as objects to be used for others' pleasure.

This is why feminist theory demands a redefinition of consent that transcends physical boundaries and includes control over digital representations. Consent, then, in feminist law, is not a fixed, one-off permission but an ever-present, contextual process based on respect and the acknowledgement of bodily and personal autonomy. All of this Deepfake pornography undermines. Even in the absence of any physical contact, it still infringes the person's embodied self through digitally simulated intimacy and exposure without consent. Feminist philosophers such as Drucilla Cornell[59] and Anita Allen[60] have long emphasised that autonomy not only relates to the freedom to deny others entry into our bodies but also to the ability to control how we are perceived, comprehended, and portrayed. The law does not recognise the virtual aspect of consent, thereby reinforcing the patriarchal assumption that a woman's image belongs to the public sphere. Subject to manipulation so long as it does not breach certain narrow legal bounds. This omission disproportionately hurts women and marginalised genders, whose bodies are already excessively exposed and commodified in digital society.

In light of this, the idea of informed consent[61], a term pioneered by feminist privacy researchers, presents itself as a necessary tool for taking back control of one's online self. Informational consent acknowledges that in a world where identities are fractured and reproduced through digital realms, people need to have a right to control not only what is being done to

[56] Leslie Francis, ‘Feminist Philosophy of Law’ in Edward N Zalta and Uri Nodelman (eds), *The Stanford Encyclopedia of Philosophy* (Summer 2025, Metaphysics Research Lab, Stanford University 2025) <https://plato.stanford.edu/archives/sum2025/entries/feminism-law/>.

[57] CATHARINE A MacKINNON, *Only Words* (Harvard University Press 1993) <http://www.jstor.org/stable/j.ctvjk2xs7> accessed 18 June 2025.

[58] Mari J Matsuda, ‘Beside My Sister, Facing the Enemy: Legal Theory out of Coalition’ (1990) 43 Stan. L. Rev. 1183.

[59] Drucilla Cornell, ‘Autonomy Re-Imagined’ (2003) 8 Journal for the Psychoanalysis of Culture and Society 144.

[60] Anita L Allen (ed), *Uneasy Access: Privacy for Women in a Free Society* (Rowman & Littlefield Publishers 1988).

[61] Anja Kovacs and Tripti Jain, ‘Informed Consent-Said Who? A Feminist Perspective on Principles of Consent in the Age of Embodied Data’ [2020] A Feminist Perspective on Principles of Consent in the Age of Embodied Data (November 2020).

their bodies but also the way their identities are constructed and circulated. It is firmly rooted in the care ethic of feminist ethics, which focuses on vulnerability and interdependence, recognising that individuals (especially women) experience actual harm when their online image is utilised without their permission to sexualise, shame, or degrade them. Feminist contestations of the liberal subject, which are understood as rational, disembodied, rights-holding agents, note how this model erases the lived experiences of individuals whose identities are already politicised and hyper-visible. Informational consent thus calls upon the law to factor in power disparities in online environments and establish positive obligations on institutions, creators, and platforms to mitigate the weaponisation of digital representations.

In the end, a feminist approach to law requires us to look beyond quick fixes and instead question the structural relations of power that allow deepfake pornography to thrive. It advocates for laws that put lived experience at the centre, values dignity over profit, and refuse the old binarisms of public/private, body/mind, and real/fake. In doing so, it not only better safeguards victims but also remakes justice in inclusive, empathetic, and transformative terms. Unless there is a reshaping of legal frameworks through a feminist prism, the harms of digital sexual violence will continue to be misunderstood, under-enforced, and poorly addressed.

IV. Conclusion

The spread of deepfakes, especially for the purposes of non-consensual sexually explicit content, is a chilling new frontier in technology-enabled sexual violence. This paper has demonstrated that deepfakes are not just benign or playful manipulations of digital content. They are a fundamental erosion of consent, autonomy, and dignity—especially for women, who are disproportionately harmed. The law's continued emphasis on physical harm, property interests, and tangible losses fails to address the uniquely gendered and digital nature of the harm that deepfakes produce. This neglect stems from a deeply embedded, male-centric legal tradition that has historically under-recognised harms inflicted through shame, reputational injury, or violations of sexual agency—forms of harm that feminist scholars have long argued must be given equal weight.

The spread of deepfakes, specifically sexually explicit and non-consensual deepfakes, represents a profoundly disturbing development in digital abuse. These technologically advanced creations of artificial intelligence, though advanced in terms of technology, represent an ethically and socially retrograde development, extending traditional forms of gendered violence into new and deceptive forms. The appearance of deepfake pornography, nearly exclusively aimed at women, unveils the patriarchal foundations of both digital culture and the current legal system. Whereas the victims are primarily women, the law still lags behind, crafted by traditional assumptions that give more importance to physical, concrete injury than to emotional, reputational, or psychological harm. This is a male construction of autonomy in which bodily invasion only counts when it involves physical invasion and not when it takes place through digital duplication and manipulation of one's face.

Even as there is an unmistakable infringement of autonomy and consent, existing Indian legal provisions are poorly placed to confront deepfake pornography efficaciously. The Information Technology Act and the Indian Penal Code were not created to deal with synthetic media or the complex realities of digital consent. These provisions bank almost exclusively on worn ideas of obscenity, defamation, or impersonation and do not reflect the particular harms of digitally manipulated intimate content. Additionally, enforcement is still sluggish, unavailable, and hampered by jurisdictional limitations, particularly when criminals act anonymously or from overseas. Victims are, therefore, left without substantive legal remedies, while platforms and intermediaries remain with minimal accountability and little proactive responsibility.

Globally, the United Kingdom and South Korea, among other nations, have taken great leaps by enacting laws criminalising not only the sharing but also the production and possession of sexually explicit deepfakes. Such laws acknowledge the severity of harm caused and impose the responsibility of detection and removal on platforms and shift towards a more feminist approach to understanding harm. Conversely, the United States still struggles with constitutional limits, specifically on freedom of speech, that complicate the regulating of deepfakes in a holistic manner. Regardless, recent federal laws like the "Take It Down" Act represent a move toward acknowledging digital consent as well as offering avenues for victims to pursue remedies.

Feminist legal theory insists on a shift in legal norms that prioritises the lived experiences of the victims of these harms. Consent needs to be understood not just as bodily permission but as including control of one's digital image and identity. Informational consent as a concept needs to be ingrained in law, realising that identity is no longer located within the physical body but is distributed between digital sites, images, and data. The unauthorised use of a person's image in sexually explicit contexts—be it in photographs or computer-generated form—must be noted as a serious infraction of autonomy and dignity no less meaningful than physical sexual violence.

Legal change needs not just criminalise the acts but also establish victim-centred processes that respect survivors' anonymity, provide for rapid removal of content, and hold both producers and distributors to account. Aside from punitive action, there needs to be a wider cultural change that questions the normalisation of deepfake pornography and challenges the cultural attitudes that make women's bodies publicly available and digitally reproducible. It also involves bringing the platforms and AI firms under greater ethical and regulatory scrutiny, forcing them to design safeguards for the very technologies they are using to harm people.

In summary, deepfake pornography is not an outre technological abuse but rather a symptom of more profound systemic flaws—legal, cultural, and technological—exposing entrenched gender hierarchies. Any serious endeavour to control deepfakes has to start by reassessing the way the law thinks about harm, consent, and autonomy in the digital era. Feminist legal theorising provides the critical eye to see these violations not as singular occurrences but as part of a continuum of patriarchal domination that now passes through machines. The future of justice online must be anchored in dignity, equity, and uncompromising commitment to protecting the full range of personal agency—both the physical and the digital.

STATEMENT OF REFERENCES

1. ‘75% Indians Have Viewed Some Deepfake Content in Last 12 Months, Says McAfee Survey’ *The economic Times* (25 April 2024)
2. Allen AL (ed), *Uneasy Access: Privacy for Women in a Free Society* (Rowman & Littlefield Publishers 1988)
3. Basu SB and Manda DP, ‘Generative Artificial Intelligence – India’s Attempt at Controlling “Deepfakes”’ (*Chambers and Partners*) <https://chambers.com/legal-trends/controlling-deepfakes-in-india>
4. Bhuptani PH and others, ‘Pornography Use, Perceived Peer Norms, and Attitudes Toward Women: A Study of College Men.’ (2024) 19 American journal of sexuality education 280
5. Brigham NG and others, ‘“ Violation of My {body:}” Perceptions of {AI-Generated} Non-Consensual (Intimate) Imagery’, *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)* (2024)
6. Burkell J and Gosse C, ‘Nothing New Here: Emphasizing the Social and Cultural Context of Deepfakes’ [2019] First Monday
7. Choudhary K and Rajpal M, ‘CRIMINALIZING DEEPFAKE TECHNOLOGY IN INDIA: A LEGAL ANALYSIS OF PRIVACY AND REGULATORY GAPS’ [2025] INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

8. Cornell D, ‘Autonomy Re-Imagined’ (2003) 8 Journal for the Psychoanalysis of Culture and Society 144
9. Dang B, Riedl MJ and Lease M, ‘But Who Protects the Moderators? The Case of Crowdsourced Image Moderation’ [2018] arXiv preprint arXiv:1804.10999
10. Datta A and Banerjee S, ‘Unmasking Deepfakes-A Legal Perspective’ (2023) 4 Jus Corpus LJ 336
11. De Souza N, ‘The Nth Room Case and Modern Slavery in the Digital Space’ *The interpreter* (Lowy Institute, 20 April 2020) <https://www.lowyinstitute.org/the-interpreter/nth-room-case-modern-slavery-digital-space>
12. Department for Science, Innovation and Technology, and Ministry of Justice, ‘Crackdown on Intimate Image Abuse as Government Strengthens Online Safety Laws’ *Gov.UK* (13 September 2024)
13. Elliott V, ‘Celebrity Deepfake Porn Cases Will Be Investigated by Meta Oversight Board’ [2024] *WIRED* <https://www.wired.com/story/meta-oversight-board-deepfake-porn-facebook-instagram/?utm_source=chatgpt.com>
14. Francis L, ‘Feminist Philosophy of Law’ in Edward N Zalta and Uri Nodelman (eds), *The Stanford Encyclopedia of Philosophy* (Summer 2025, Metaphysics Research Lab, Stanford University 2025) <https://plato.stanford.edu/archives/sum2025/entries/feminism-law/>
15. Garver R, ‘California Laws Target Deepfake Political Ads, Disinformation’ [2024] *Voa News* <https://www.voanews.com/a/california-laws-target-deepfake-political-ads-disinformation/7789746.html>
16. Hogan Lovells IL, ‘BRIEFING PAPER: DEEPFAKE IMAGE-BASED SEXUAL ABUSE, TECH-FACILITATED SEXUAL EXPLOITATION AND THE LAW’ <https://equalitynow.org/resource/briefing-paper-deepfake-image-based-sexual-abuse-tech-facilitated-sexual-exploitation-and-the-law/>
17. Holland Michel A, ‘The ACLU Fights for Your Constitutional Right to Make Deepfakes’ *WIRED* (24 July 2024)
18. Hornstein O, ‘Tech Minister on Regulating Big Tech and Tackling Online Hate’ (*UK TECH NEWS*, 26 August 2024) <https://www.uktech.news/news/government-and-policy/tech-minister-on-regulating-big-tech-and-tackling-online-hate-20240826?>
19. Hsu T, ‘Deepfake Laws Bring Prosecution and Penalties, but Also Pushback’ *NY Times* (22 May 2025) <https://www.nytimes.com/2025/05/22/business/media/deepfakes-laws-free-speech.html>
20. ‘Increasing Threat of DeepFake Identities’ <https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf>
21. Jha S, ‘“Remove Misinformation, Deepfakes within 36 Hrs”: Centre to Social Media Firms’ *India Today* (7 November 2023) <https://www.indiatoday.in/india/story/remove-misinformation-deepfakes-within-36-hrs-centre-to-social-media-firms-2460129-2023-11-07>
22. Kadem D and Lassouane KME, ‘The Negative Impact of Deepfake Technology on the Reputation of Prominent Figures on Social Media Platforms: An Analytical Study on a Sample of Fabricated Videos.’ (2024) 4 Journal of Science and Knowledge Horizons 510
23. Karagianni A and and MD, ‘A Feminist Legal Analysis of Non-Consensual Sexualized Deepfakes: Contextualizing Its Impact as AI-Generated Image-Based Violence under EU Law’ (2024) 0 Porn Studies 1
24. Kira B, ‘Deepfakes, the Weaponisation of AI Against Women and Possible Solution’ (*Verfassung*, 3 June 2024) <https://verfassungsblog.de/deepfakes-ncid-ai-regulation/>
25. Kovacs A and Jain T, ‘Informed Consent-Said Who? A Feminist Perspective on Principles of Consent in the Age of Embodied Data’ [2020] A Feminist Perspective on Principles of Consent in the Age of Embodied Data (November 2020)
26. MacKINNON CA, *Only Words* (Harvard University Press 1993) <http://www.jstor.org/stable/j.ctvjk2xs7> accessed 18 June 2025
27. Martin N, ‘Image-Based Sexual Abuse and Deepfakes: A Survivor Turned Activist’s Perspective’ [2021] The Palgrave Handbook of Gendered Violence and Technology 55

28. Matsuda MJ, ‘Beside My Sister, Facing the Enemy: Legal Theory out of Coalition’ (1990) 43 Stan. L. Rev. 1183
29. Ministry of Justice and Davies-Jones MP A, ‘Government Crackdown on Explicit Deepfakes’
30. NGUYỄN T, ‘California Governor Signs Bills to Protect Children from AI Deepfake Nudes’ *AP News* (30 September 2024) <https://apnews.com/article/ai-deepfakes-children-abuse-7dcf5c566e2a297567f1e148ac2074a4>
31. Nover S, ‘South Korea Banned Deepfakes. Is That a Realistic Solution for the US?’ *GZero* (8 October 2024) <https://www.gzeromedia.com/gzero-ai/south-korea-banned-deepfakes-is-that-a-realistic-solution-for-the-us>
32. Öhman C, ‘Introducing the Pervert’s Dilemma: A Contribution to the Critique of Deepfake Pornography’ (2020) 22 Ethics and Information Technology 133
33. ——, ‘Introducing the Pervert’s Dilemma: A Contribution to the Critique of Deepfake Pornography’ (2020) 22 Ethics and Information Technology 133
34. Okolie C, ‘Artificial Intelligence-Altered Videos (Deepfakes), Image-Based Artificial Intelligence-Altered Videos (Deepfakes), Image-Based Sexual Abuse, and Data Privacy Concerns Sexual Abuse, and Data Privacy Concerns’ (2023) 25 Journal of International women’s studies <https://vc.bridgew.edu/jiws/vol25/iss2/11?utm_source=vc.bridgew.edu%2Fjiws%2Fvol25%2Fiss2%2F11&utm_medium=PDF&utm_campaign=PDFCoverPages>
35. Ren S and others, ‘Do Deepfake Detectors Work in Reality?’ [2025] arXiv preprint arXiv:2502.10920
36. Reuters, ‘South Korea to Criminalize Watching or Possessing Sexually Explicit Deepfakes’ *CNN* (26 September 2024) <https://edition.cnn.com/2024/09/26/asia/south-korea-deepfake-bill-passed-intl-hnk>
37. Robertson A, ‘Virginia’s “Revenge Porn” Laws Now Officially Cover Deepfakes’ *The Verge* (2 July 2019) <https://www.theverge.com/2019/7/1/20677800/virginia-revenge-porn-deepfakes-nonconsensual-photos-videos-ban-goes-into-effect>
38. Roscoe J, ‘Deepfake Scams Are Distorting Reality Itself’ [2025] *WIRED* <https://www.wired.com/story/youre-not-ready-for-ai-powered-scams/>
39. Sabin S, ‘Deepfakes Are Easy to Make, but Also Easy to Detect’ (*Axios*, 12 August 2024) <https://www.axios.com/2024/08/12/def-con-darpa-deepfake-lab?>
40. Schaden V L, ‘Brooke Monk Leaks: Unpacking The Viral Rumors And Digital Footprint’ (*Procamp*) <https://www.procamp.qa/tiktoknews-007/brooke-monk-nude-leaks/>
41. Seng S, *Rape Culture in Media Coverage: An Analysis of the" Nth Room" Scandal* (2024)
42. Shankar V, ‘Deepfakes Call for Stronger Laws’ *The Hindu Business Line* (16 July 2023) <https://www.thehindubusinessline.com/business-laws/deepfakes-call-for-stronger-laws/article67077019.ece>
43. Suslavich BT, ‘Nonconsensual Deepfakes: A" Deep Problem" for Victims’ (2023) 33 Alb. LJ Sci. & Tech. 160
44. ‘The Tensions of Deepfakes.’
45. Umbach R and others, ‘Non-Consensual Synthetic Intimate Imagery: Prevalence, Attitudes, and Knowledge in 10 Countries’, *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (2024)
46. Wood G, ‘Disinformation and Deepfakes: Countering Gender-Based Online Harassment’ (*Center for strategic and International studies*) <https://www.csis.org/events/disinformation-and-deepfakes-countering-gender-based-online-harassment>
47. Yasar K, Barney N and Wigmore I, ‘What Is Deepfake Technology?’ (*Tech Target*, 22 May 2025) <https://www.techtarget.com/whatis/definition/deepfake>
48. Yoon M, ‘“Anti-Nth Room” Legislation, an Unfulfilled Promise’ *The Korea Herald* (11 July 2022) <https://www.koreaherald.com/article/2909004>
49. Indian penal code 1862
50. Indian Penal Code 1862
51. Information Technology Act, 2000

*****