IJAR&D
Peer-reviewed | Open Access

International Journal of Academic Research and Development (IJAR&D)
ISSN : 2395-1737 (Print), Volume 12, No. 3, Page No 22-29
DOI : https://doi.org/10.70381/23951737.v12.js3.2026.3
A Quarterly Journal Published by Bharti Publications, New Delhi, India

Non Consensual Deepfakes: A Gendered Analysis of Legal Gaps and Remedies

Kalpna Sharma

Assistant Professor, Law Center II, Faculty of Law, University of Delhi, Delhi

Suneel Kumar

Professor, Department of Commerce, Shaheed Bhagat Singh College, University of Delhi, Delhi

Nazia

Research Scholar, Department of Management, Central University of Himachal Pradesh, Delhi

Abstract

Purpose: Deepfake technology has evolved to the point of producing hyper-realistic fake media, and it has been abused to the extreme, with the creation of intimate images without the consent of the subjects. At the international level, some countries are hurriedly drafting legislation to address deepfake- related misuse, while the existing framework is disjointed and ill- equipped to tackle the gender- specific problems. The purpose of this paper is to trace the boundaries of the existing legislation and the main shortcomings in safeguarding against deepfakes from a gender perspective and assess existing remedies and their effectiveness for women victims.

Approach: This paper systematically analyzes the scholarly and grey literature related to deepfake regulation by mapping key elements of existing laws. It identifies the gaps that still need to be addressed from a gender perspective and further evaluates the effectiveness of available remedies for women victims.

Findings: Literature analysis shows five major gaps: the absence of comprehensive and country-specific criminal laws, the ineffective regulation of traditional torts and privacy laws, lack of platform liability frameworks and practices of moderating platform content, lack of legislator-centered approaches in supporting victims (including anonymous reporting, legal assistance, and compensation when they have suffered harms). The current work of Parliament in combating gender-based violence is structurally inadequate to overcome gender-based violence assisted by deepfakes. A model criminalization law for non-consensual intimate synthetic imagery with an explicit, gender-driven approach, proactive takedown commitments imposed on intermediaries, dedicated cybercrime teams for the support of victims of such crimes, and international harmonization of the law through a binding convention are the practical recommendations at the end of the paper.

Keywords: *Deepfake, Gender- Based Violence (GBV), Non- Consensual Videos, Legal Aspects, Artificial Intelligence-Based Victimization*

1. Introduction and Literature Review

Artificial Intelligence (AI), computer vision, and generative open-source software have created an increased ease of creating deepfakes, which includes the formation of fake audio, images, and videos of individuals either articulating or acting out content they never performed (Chesney & Citron, 2019). Hyper-realistic fake media has come into existence with the use of deepfake technology, where intimate images are produced without the consent of the person (Citron, 2019; Henry et al., 2020). This technology is mainly used for enjoyment, education, and accessibility, where a large amount of money and power are associated with

creating deepfakes (Farid, 2021). This technology is more of an unsettling and frightening change for women than for men (Gosse & Burkell, 2020). The UN Women (2025) press release adds to the information that about 90 to 95% of all online videos are women's pornographic videos, which are non-consensual in nature. Celebrities, journalists, political activists, and the population at large are frequent victims of deepfakes as they are mainly targeted, humiliated, blackmailed, and even silenced (Maddocks, 2020). This is an extreme manifestation of technology that facilitates sexual violence, reinforcing the dynamics of inequality (Henry & Powell, 2018). This negative change impacts women's autonomy, dignity, and ability to participate in digital contexts (Franks, 2019).

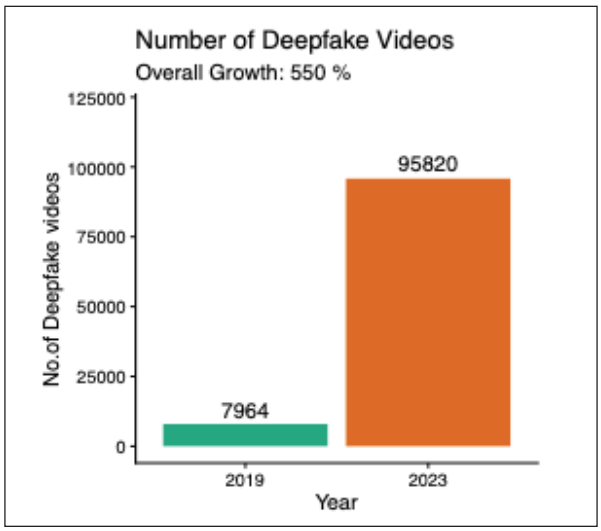


Figure 1: The Growth of Deepfake Videos

Source: Author's own compilation (Data Source: Security Hero, 202 https://www.securityhero.io/state-of-deepfakes/)

Figure 1 shows a 550% growth rate of 550% in the formation of deepfake videos from 2019 to 2023. This exponential increase in deepfake videos over a four-year span is the outcome of free and affordable access to AI models. This sudden jump in number is an alarming call to different countries and their governments to regulate the usage of deepfake creations (Robertson, 2023). The strict rules by the government can avoid victimization, blackmail, and specifically Gendered Based Violence (GBV) (McGlynn & Rackley, 2023).

Various governments work on increasing public awareness, but the legal systems of the world have lagged behind deepfake technology (Robertson, 2023). The initial legislation only targeted revenge porn, which means real porn photos or videos without consent (McGlynn & Rackley, 2017). The situation is far more complex with deepfakes, as the person creates the content to mock and does not engage in producing the original sexual images (Chesney & Citron, 2019). The harm it causes can be identical to real images. This content is both easily and quickly spread at a large scale in a fraction of a second, but it is hard to prove that it is fake (Citron & Franks, 2014; Flynn et al., 2021). Many general laws, including defamation law, copyright law, and anti-harassment laws, do not describe these circumstances or provide any particular punishment. The victims of deepfakes are left with no remedy for these heinous acts. Moreover, there are significant differences in legislation across jurisdictions (Hamilton, 2024). In some countries in the Global North, including South Korea, new bills and concepts have been introduced specifically for this field, whereas in many countries in the Global South, legislation is completely absent (Naik & Choudhury, 2023).

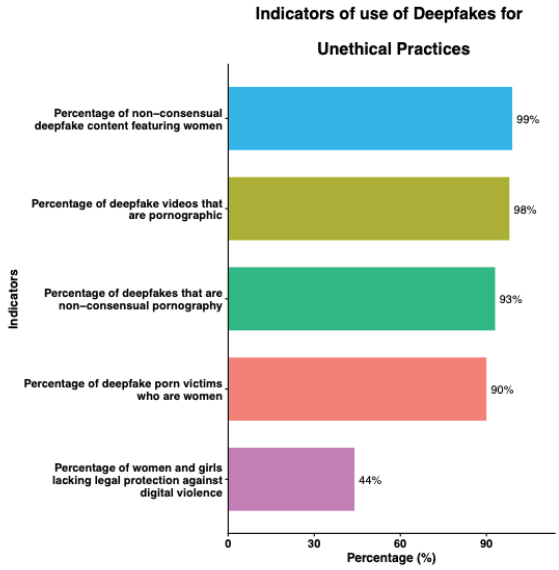


Figure 2: Indicators Showing Unethical Use Deepfake Videos

Source: Author's own compilation

(UN Women, 2026 https://www.unwomen.org/en/articles/explainer/when-justice-fails-why-women-cant-get-protection-from-ai-deepfake-abuse)

(UN Women, 2025 https://www.unwomen.org/en/news-stories/press-release/2025/11/digital-violence-is-intensifying-yet-nearly-half-of-the-worlds-women-and-girls-lack-legal-protection-from-digital-abuse)

Figure 2 highlights different indicators of misuse of Deepfake videos, which are unethical but not illegal due to the non-existence of centralized law. The graph shows that 98% of videos are pornographic deepfakes, and women are victims in 90% of deepfake videos. It reflects

the importance of GBV laws to protect women who are facing mental trauma and blackmail from non-consensual deepfake pornography videos (UN Women, 2025). If we only consider non-consensual deepfake pornography videos, the number is 93%, of which women featured in videos are 99% (Deeptrace, 2019). This is the main area that needs to be addressed with legal enforcement. Also, UN Women (2025) press release, highlights that despite various judicial steps for controlling digital violence against women in many countries, 44% of women lack these legal protections. This is caused by negligence in enforcement and by a non- supportive environment provided by police, judges, and society's mindset. This happens because they are not open to confronting such problems or have a closed mindset of hiding the situation, due to family pressure to avoid the reputational damage. Another reason is that they are illiterate in legal matters and do not understand their rights and remedies in resisting such acts of violence (Naik & Choudhury, 2023).

Few studies have systematically studied the patchwork of global laws and regulations on deepfakes in a systematic way, but none of them have performed the research explicitly with a gender lens (Henry & Powell, 2018). Previous studies offer analysis of specific laws and propose legislation that regulates deepfakes, but they lack the inclusion of a gender perspective in their studies. This study fills these gaps by summarizing and discussing the current laws and policies that afford protection to women against deepfake's misuse (McGlynn et al., 2021). The study aims to identify the legislative and regulatory flaws with respect to the non-consensual creation and distribution of synthetic intimate images that pose risks for women. It also provides measures to address these flaws.

2. Research Objectives

The research focuses on the overall research question and includes answers to these questions

- To identify doctrinal, procedural and structural inadequacies in current legal safeguards that are particularly detrimental to the rights of women victims in a systematic way.
- To assess whether platform governance mechanisms and cross-border enforcement mechanisms are sufficient in mitigating the spread and impact of gendered deepfakes.
- To connect and gather together academic insights and suggest a coherent group of legal and policy changes that would place a gender-inclusive and victim-driven framework that is in tune with deepfake regulation.

3. Discussions of the Study

The literature review shows that the legal landscape in the world is fragmented and systemic towards women's protection against deepfake-facilitated abuse. The gaps are not technical issues but conceptual, as our study suggest a lack of alignment between concepts of law and digital gendered harm. The five emergent areas of gap are discussed in Table1.

3.1 The Legislative Vacuum (no criminal prohibitions for technology- specific crimes)

Table 1: Current status of Deepfake laws in various countries

Jurisdiction	Legal Mechanism	Identified Lacuna in existing legal mechanisms
South Korea	Special Act on the Punishment of Sexual Violence Crimes Using Deepfake Technology (2020) (Kim & Lee, 2022)	It prohibits the creation, distribution or possession of deepfakes, with a sentence of up to 5 years of imprisonment or a fine for those who violate the prohibition, which does not exist in other countries in the world (Kim & Lee, 2022).
United States	Non- integrated state laws in USA (California, New York, Texas, Virginia, Georgia), the Deepfakes Accountability Act is proposed (Hamilton, 2024).	There is no centralized federal law, and more than 30 states have no specific law, and the proposed federal law has been languishing (Hamilton, 2024).
United Kingdom	Online Safety Act 2023	The provision was introduced late and criticized for being weak in limiting the scope of intimate deepfakes and in terms of the enforcement mechanisms (McGlynn & Rackley, 2023).
India	Information Technology Act (Sections 66E and 354C)	Totally inadequate as it lacks reference to synthetic creation, consent to likeness or to the special psychological harms (Bhandari, 2023).

European Union	Digital Services Act (DSA)	Makes efforts to include due diligence in platforms but does not attempt to align substantive criminal law in member states (Tene & Polenetsky, 2023; Wanger & Janssen, 2022).

Source: Author's own compilation

The most basic shortfall is that there are no laws in place that explicitly outlaw the creation or sharing of intimate deepfakes without consent. As early as the beginning of 2026, a handful of states have framed such laws. Special Act on the Punishment of Sexual Violence Crimes Using Deepfake Technology (2020) by the Republic of Korea (South Korea) continues to set the global standard for the punishment of creation, distribution, and even possessing deepfake pornography, with up to 5 years imprisonment and/or large fines (Kim & Lee, 2022). In the United States of America (USA), there are varying types of legislation addressing the issue of non-consensual synthetic intimate images, with California, New York, Texas, Virginia, and Georgia having legislation in place and more than thirty states lacking specific non-consensual synthetic intimate image legislation (Hamilton, 2024). Furthermore, there is no centralized and single federal U.S. legislation. The proposed Deepfakes Accountability Act has been stuck in Congress since 2019, with limited and uncertain application to synthetic content and the Shield Act is more about real intimate images, and whether it will apply to synthetic images remains uncertain (Chesney & Citron, 2019; Farid, 2021).

But even in many European countries, there are no clear laws on deepfakes. The legislation was drafted before the end of the parliamentary process and has been condemned as being ineffective, with weak enforcement and limited scope, as it criminalizes the sharing of intimate deepfake images without consent in the United Kingdom (UK) only (McGlynn & Rackley, 2023). The EU's Digital Services Act (DSA) prescribes due diligence requirements for these platforms without introducing any uniformity in terms of criminal law protection for deepfake abuse, meaning there remains a piecemeal approach in terms of substantive criminal law (Tene & Polenetsky, 2023; Wanger & Janssen, 2022). In India, the protection provided by Section 66E of the Information Technology Act (privacy violation) and Section 354C (voyeurism) have failed to be effective as they do not cover synthetic creation, consent with respect to one's likeness or psychological harm caused by manipulated sexual imagery (Bhandari, 2023). When legislation lacks this safety, the women have no alternative but to suffer abuse without remedy or to try and fit their experience into general legislation, often with little success.

3.2 The Remedial Mismatch by over-reliance on traditional legal doctrines

Table 2: Lacunas in Traditional Torts

Traditional Tort	Requirements	Lacuna in traditional Tort in Deepfake Application
Defamation	False statement of fact that hurts someone's reputation.	Requires forces to have to fight for authenticity (secondary trauma) and rejects injury of dignity/ autonomy (Citron & Franks, 2014).
Privacy Torts	Assumes that the disclosed private information is true.	Provides no type of legal protection when the imagery is not based on real events/situations but purely fictional/fabricated (Burkell & Gagne, 2021).
Intentional Infliction of Emotional Distress	Sets an extremely high bar for severe emotional harm and outrageous conduct.	But for non-celebrity victims, their suffering can be denied by law, typically because it is not noticed, and often they do not have access (Citron, 2019).
Copyright Law	Protects the person who is the owner of Intellectual property rights.	It is extremely rare that the victim owns the rights to the deepfake, and its use further contributes to the victim being treated as a commodity (Brown & Sinclair, 2022).
Harassment & Stalking	Requires a targeted pattern of conduct directed at a specific victim.	Does not plan for an around-the-world viral video (Flynn et al., 2021).

Source: Author's own compilation

Table 2 shows the Remedial Mismatch by over-reliance on traditional legal doctrines. It identifies the absence of specific legislation addressing deepfakes. The victims of a deepfake rely upon either a tort claim like intentional infliction of emotional distress, stalking, invasion of privacy/false light or criminal complaints for harassment, copyright, or defamation. The evolution of deepfakes and the lack of consensus on how to differentiate between their specific forms make it impossible to calculate how much harm they cause. As deepfake attacks evolve and there is no agreement on distinguishing them, it is impossible to estimate the harm or results they inflict (Franks, 2019; Citron, 2019; McGlynn et al., 2021).

Firstly, defamation involves an incorrect statement about a fact which hurts someone's goodwill. Deepfakes are created, but when proving the falsity of a sexualized

image in court, the person has to fight to defend the authenticity of the content, thus subjecting herself to what amounts to a second trauma. Furthermore, defamation does not compensate or justify any injury to another person's dignity and autonomy from having their likeness used for sexual exploitation, even if it has no focus on reputation (Gillespie, 2022). Secondly, privacy laws such as public disclosure of private facts assume the information is accurate; in the case of synthetic imagery, this is clearly not the case (Burkell & Gagne, 2021). Thirdly, intentional infliction of emotional distress requires outrageous conduct and severe emotional harm, which is an extremely high standard and would likely not be satisfied with the findings of courts for victims that are not celebrities. Third, intentional infliction of emotional distress is a very high standard to meet for the element of outrageous conduct and the element of severe emotional harm, which would likely not be met by those who are non-celebrity victims, and the courts have attempted to limit the standard. Fourth, copyright law can be utilized at times although the depicted person does not often have copyright in the deepfake, yet it is not enough to surpass personal dignity-infringing violations and could carefully reinforce the belief that the person's image is a retail.

Patterns of conduct that may be required by criminal harassment and stalking laws often aren't satisfied by a single posting of a deepfake video onto the internet that gets spread around the world. Moreover, a large number of U.S. states and the UK (Criminal Justice and Courts Act 2015, section 33) have revenge porn statutes based on the notion of private sexual photographs that are initially produced consensually, which is an explicit or implied exclusion of entirely reconstituted materials (McGlynn & Rackley, 2017; Flynn et al., 2021).

1.4 The limited ability of the platform to handle content liability issues and inadequate content moderation

Where substantive laws exist, the effectiveness of these can only be realized when there is the will and ability to rapidly take down deepfake content from online platforms (Wittes, 2021). The literature continues to show that there is a major lack of accountability. The Congressional concept of giving liability protection to platforms when users are creating content and the congressional intention of not making it easier for others to be responsible for that content are likely to remain intact under Section 230 of the Communications Decency Act (Citron & Wittes, 2017). While many third parties want to be responsible for the content of platforms, Congress is unlikely to make it easier to hold them liable. While there are plans to enforce duty of care obligations on DSA in Europe and new proposals for the same in the U.S., there is not yet a proactive approach (Wagner & Janssen, 2022). However, there are user flagging systems in place that enable major platforms to detect deepfakes, which the victim needs to use is far from efficient and often emotionally draining, as it comes back from one platform to another (Wittes et al., 2021).

Research shows that deepfake photos of women are generally found on nudification websites and on less regulated web platforms that victims have less power over (Deeptrace, 2019). But when it comes to removing images that are not shared with consent, there are inconsistencies on general platforms such as Meta and Google, and it is often impossible to remove such content within the time frame in which it goes viral (Fiesler et al., 2022). Deepfake variations can escape perceptual hashing, which is a feature that has made hash-based detection technologies heterogeneous and not yet suitable for this type of variation (Marra et al., 2019). Deepfake variations can get out of perceptual hashing; currently, hash-based detection technologies are not adapted to this type of variation. It creates a constant whack-a-mole situation; every time the woman's image is used, there is hardly any sanction on the platform. This feeds into a never-ending whack-a-mole situation wherein the images of a woman can be misused infinitely with little to no platform penalties.

1.5 Jurisdictional Fragmentation and Cross-Border Enforcement Barriers

Globally, Deepfake abuse is a culprit in many countries. A can transfer a clip using a victim's face from country B, store it on a server in country C, and share it on social networks around the world. This literature review confirms the significant constraints of territorial criminalization in challenging this situation (Svantesson, 2020). The existing and outdated mutual legal assistance treaties (MLATs) are slow, costly, and inadequate to the volume and velocity of cybercrime. Budapest Convention on Cybercrime is a body of law which establishes a framework for international cooperation; however, there is a significant number of countries, including most influential source countries, which have not ratified the Convention, and the provisions of the Convention regarding computer-generated fraud or offenses against the secrecy, integrity and availability of computerized data do not explicitly cover image-based sexual abuse (UN Special Rapporteur on violence against women, 2021).

The soft law, which has been used thus far to harmonize the law and to generate awareness, but not to compel changes in legislation, such as the Special Rapporteur on the situation of women in the enjoyment of all civil, political, economic and social rights on violence against women online (2021). The European Union framework

in the battle against child sexual abuse is a precedent for a regime of reporting and detection, but no such all-encompassing framework for non-consensual intimate deepfakes of adults seems to exist, leaving adult women off the list of victims. The number of people that call for a historically specific GBV technology-based violence treaty is increasing, but there is not yet a political consensus (McGlynn & Rackley, 2023).

1.6 Neglect of Victim-Centered Approaches and Gendered Impact

Broad-brush stroke view of deepfake legislation that lacks gender sensitivity and fails to identify gendered aspects and root causes of harm is a common theme across the literature. As shown in the data in Figure 2, there is a higher prevalence of deepfake violence among women compared to men and the prevalence of deepfake violence among women is significantly higher. The use of deepfakes in GBV and gender misogyny is not included in the vast majority of legislation, as it does not include the use of deepfakes as an act of gender-based violence or gender misogyny (Henry & Powell, 2018). This lack of legal framing has had real-life consequences. Discovery demands by the parties via legal proceedings are one way that perpetrators can use to harass the victim. Few statutes allow anonymous reporting of perpetration to ensure that the victim is not further harassed by discovery demands. Second, legal aid and psychological assistance are limited, and women have no promise of a successful outcome in civil litigation, and they may have to pay out-of-pocket costs. Lastly, criminal sentencing norms are only beginning to consider the particular ways in which the use of deepfakes against women to create pornography has unique, shaming, and silencing effects on women's role in public discourse, particularly shutting down the voices of journalists, politicians, and activists (Amnesty International, 2021).

Additionally, no protective order or takedown system helps women protect themselves from the digital footprint of these racist deepfake images, which can crop up years later, therefore always endangering their online reputation (Smith & Dyer, 2024). There is some relief with the right to be forgotten as written in the EU GDPR, yet with a slim amount of reach, as this does not apply to the entire web, and only to particular content providers (Van der Sloot & Zuiderveen Borgesius, 2021). Together, these make up a hostile digital environment, and even an "image of chill" on women's right to freedom of association or freedom of expression due to the misuse of deepfakes.

4. Conclusion of the Study

This systematic review underscores the serious shortcomings of the legal status of women's rights to protection from sexual abuse facilitated by deepfakes. These gaps include legislative silence, doctrinal gaps, platform immunity, jurisdictional chaos, and failure to focus on the victims. These aren't just holes in something but are part of a more fundamental problem where they appear not to consider synthetic imagery of the sexual kind as an incitement to violence of the same nature as physical sex-related violence and therefore treat it with the same legal gravity. If the law does not encompass full reform, it will further leave digital areas open for abusers and further reinforce the inequalities that it is meant to cure.

5. Suggestions for Reform

- ***Adopt a comprehensive model criminal law:*** Legislation should make clear the punishment for sharing, distribution, and threatened sharing of sexualized images, images of private parts of the body without consent because doing so is a sufficient violation of autonomy and dignity (Whitten, 2023). The law should cover either real or imagined content, eliminate the intent loophole that exists in many harassment laws, and add extraterritorial jurisdiction provisions for the victim, or to include when the content is in the state where the harm is done (Delfino, 2020).
- ***Compulsory Platform Responsibility:*** There should be well-established hashing and AI detection means to be rigorously used on Internet platforms to identify and remove deepfake intimate images at the primary stage of a user's creation, with strict penalties in case of failure. Repeated uploads will have to be prevented by requiring what is known as a "notice-and-stay-down" procedure rather than a "notice-and-takedown" procedure. Platforms should automatically report plainly verified incidents to police and retain evidence.
- ***Enforce Victim-Centered Support Ecosystems:*** State-funded cybercrime, specific dedicated expertise and services to support victims with expedient takedown support, line-of-sight free psychological counselling, free legal support counselling, and anonymous reporting portals. Civil actions should also include the award of statutory damages, an injunction, and pseudonymous litigation to protect the anonymity of victims.
- ***Multilateral international legal harmonization:*** A binding multilateral legal harmonization is required for technology-specific GBV, which can be inspired by the Budapest Convention but have substantive provisions relating to deepfake abuse. The convention would set the minimum standards

for criminalization, mutual legal assistance, and cross-border cooperation, thus overcoming the shortcomings of bilateral MLATs.

- ***Ensure a Gender Lens in All Legislation***: To involve women's rights groups, digital feminists and survivors in legislation (Patella- Rey, 2022). Every planned bill on cybercrime or online security should include a Gender Impact Assessment that internalizes and takes steps to eliminate the power anomalies that are the subject of abuse by deepfakes. The implementation of these suggestions will bridge the gap between technology exploitation and the protective role of law. Women will get the freedom to enjoy their rights in a digital public sphere unprecedented in history without virtual sexual violence.

Funding Acknowledgement: The Author wants to acknowledge that this research paper is a part of the research project funded by ICSSR, Ministry of Education, Government of India with file no. Gen -21/2021-22/ ICSSR/RP.

References

Amnesty International. (2021). Toxic Twitter: Violence and abuse against women online. Amnesty International.

Bhandari, V. (2023). Non- consensual deepfakes and Indian law: A critical analysis. Indian Journal of Law and Technology, 19(1), 1-29.

Brown, A., & Sinclair, K. (2022). Deepfake pornography and the limits of copyright remedies. Journal of Intellectual Property Law & Practice, 17(8), 645- 656.

Burkell, J., & Gagne, M. (2021). Revisiting the 'reasonable expectation of privacy' in the age of deepfakes. Canadian Journal of Law and Technology, 19(2), 135-159.

Chesney, R. & Citron, D. K. (2019). Deepfakes and the new disinformation war: The coming age of post- truth geopolitics. Foreign Affairs, 98(1), 147-155.

Citron, D. K. (2019). Sexual privacy. Yale Law Journal, 128(7), 1870-1960.

Citron, D. K. (2022). The fight for digital privacy: How to protect rights in the age of deepfakes. Harward Law Review Forum, 135(7), 361-384.

Citron, D. K., & Franks, M. A. (2014). Criminalizing revenge porn. Wake Forest Law Review, 49(2), 345-391.

Citron, D. K., & Wittes, B. (2017). The internet will not break: Denying bad Samaritans Section 230 immunity. Fordham Law Review, 86(2), 401-425.

Citron, D.K., & Frank, M. A. (2020). Evaluating the legal response to deepfake sex videos. Boston University Law Review, 100(4), 1201-1246.

Cusack, C., & Waran, K. (2021). Deepfakes and consent: A comparative analysis of Australian and UK laws. Monash University Law Review, 47(3), 689-714.

Delfino, R. A. (2020). Pornographic deepfakes: The case for federal criminalization of non- consensual synthetic intimate imagery. Fordham Law Review, 88(6), 2377-2420.

Deeptrace. (2019). The state of deepfakes: Landscape, threats, and impact. Deeptrace Labs.

Douglas, D. M. (2023). Doxing, deepfakes, and the weaponization of women's image online. Ethics and Information Technology, 25(2), Article 32.

Farid, H. (2021). Creating, using, misusing, and detecting deep fakes. Journal of Online Trust and Safety, 1(1), 1-27.

Fiesler, C., Garrett, R. K., & Beard, N. (2022). What do we do when deepfakes go viral? Platform governance gaps and gendered abuse. New Media & Society, 24(5), 1107-1125.

Flynn, A., Henry, N., & Powell, A. (2021). More than revenge: The continuum of image- based sexual abuse. Feminist Criminology, 16(4), 420-439.

Franks, M. A. (2019). The lawless internet? Myths and realities of online abuse. Columbia Journal of gender and law, 40(1), 1-45.

Gillespie, T. (2022). Do not recommend? Reduction as a form of content moderation. Social Media + Society, 8(3), 1–13.

Gosse, C., & Burkell, J. (2020). The impact of non- consensual deepfake pornography on women's willingness to engage online. Feminist Media Studies, 20(7), 1025-1041.

Hamilton, I. (2024). Deepfake porn laws in the United States: State of the states. Harward Journal of Law & Technology, 37(2), 567-612.

Henry, N., & Powell, A. (2018). Technology- facilitated sexual violence: A literature review of empirical research. Trauma, Violence, & Abuse, 19(2), 195-208.

Henry, N., McGlynn, C., Flynn, A., Johnson, K., Powell, A., & Scott, A. J. (2020). Image- based sexual abuse: A study on the causes and consequences of non- consensual nude or sexual imagery. Feminist Legal Studies, 28(1), 41-67.

Kim, S., & Lee, H. (2022). South Korea's response to digital sex crimes: The Special Act on deepfake pornography. Asian Journal of Criminology, 17(2), 153-170.

Klein, A. (2023). Deepfakes and domestic violence: Using technology to coerce and control. Violence Against Women, 29(10), 1954-1976.

Lanier, C. D., & Saint- Clair, J. (2022). The inadequacy of Section 230 in addressing synthetic intimate imagery. North Carolina Journal of Law & Technology, 24(1), 156-197.

Maddocks, S. (2020). 'A deepfake porn plot intended to silence me': Exploring continuities between pornographic and political deepfakes. Porn Studies, 7(4), 431-444.

Marra, F., Gragnaniello, D., Cozzoline, D., & Verdolivo, L. (2019). Detection of GAN- generated fake images over social networks. In Proceedings of the IEEE Conference on Multimedia Information Processing and Retrieval (pp. 384-389).

Matamoros- Fernandez, A., & Farkas, J. (2021). Racism, misogyny and the phantomization of deepfakes. Information, Communication & Society, 24(15), 2274-2291.

Mc Glynn, C. (2022). Cyberflashing, deepfakes and the law: Recognizing intimate image- based harms. Legal Studies, 42(4), 598-618.

McGlynn, C., & Rackley, E. (2017). Image- based sexual abuse. Oxford Journal of Legal Studies, 37(3), 534-561.

McGlynn, C., & Rackley, E. (2021). Beyond 'revenge porn': The continuum of image- based sexual abuse. Feminist Legal Studies, 25(1), 25-46.

McGlynn, C., & Rackley, E. (2023). The UK Online Safety Act and intimate image abuse: A missed opportunity? Journal of Media Law, 15(1), 82-101.

Naik, R., & Choudhary, S. (2023). Policing deepfake crimes against women in the Global South: Challenges and remedies. International Journal of Cyber Criminology, 17(1), 88-109.

Nair, A. (2024). Deepfakes and digital misogyny in India: A socio-legal critique. Economic and Political Weekly, 59(12), 45-52.

Patella- Rey, P. J. (2022). Beyond the pixelated body: Deepfakes and the commodification of female identity. Signs: Journal of Women in Culture and Society, 47(4), 967-988.

Paul, S., & Strinati, G. (2021). Deepfake detection and digital forensics: A gendered perspective. IEEE Security & Privacy, 19(3), 58-66.

Robertson, A. (2023). The global patchwork of deepfake legislation: A comparative study of five jurisdictions. International Journal of Law and Information Technology, 31(1), 1-28.

Rubin, V. L., & Chen, Y. (2020). Misinformation, disinformation and deepfakes: A feminist information ethics approach. Journal of Information Ethics, 29(2), 72-93.

Sikka, T. (2022). Technology- facilitated sexual violence and the Indian legal system: Gaps and the way forward. Journal of Indian Law and Society, 13(1), 89-112.

Smith, L., & Dyer, R. (2024). The right to be forgotten and deepfake intimate imagery: A European perspective. European Journal of Law and Technology, 15(1),1-18.

Stabile, C. A. (2021). The deepfake of consent: How platform capitalism normalizes gendered exploitation. Feminist Theory, 22(4), 543-560.

Svantesson, D. J. B. (2020). Solving the Internet jurisdiction puzzle. Oxford University Press.

Svantesson, D. J. B. (2022). Private international law and non-consensual deepfakes: A framework for cross- border redress. Journal of Private International Law, 18(3), 563-587.

Symantec Corporation. (2020). Deepfakes and the next wave of digital sextortion: Threat landscape analysis. Broadcom Inc.

Security Hero. (2023). 2023 state of deepfakes: Realities, threats, and impact.

Tene, O., & Polonetsky, J. (2023). The EU Digital Services Act and platform responsibility for deepfake- based harms. Berkeley Technology Law Journal, 38(1), 179-224.

Tsalikis, C. (2022). Nudification apps, gender- based violence and the need for design liability. Journal of Law, Technology & Policy, 2022(1), 99-137.

UK Home office. (2022). Tackling violence against women and girls: Strategy 2021- 2024- Progress update (CP 648). HMSO.

UN Human Rights Council. (2018). Report of the Special Rapporteur on violence against women, its cases and consequences on online violence against women and girls (A/HRC/38/47). United Nations.

UN Women. (2020). Online and ICT- facilitated violence against women and girls during COVID- 19. UN women East and Southern Africa Regional Office.

UN Women. (2025). AI-powered online abuse: How AI is amplifying violence against women and what can stop it.

UN Women. (2025). Digital violence is intensifying, yet nearly half of the world's women and girls lack legal protection from digital abuse

UN Women. (2026). When justice fails: Why women can't get protection from AI deepfake abuse.

Van der Slot, B., & Zuderveen Borgesius, F. (2021). The right to be forgotten and deepfakes: A mismatch? Information Polity, 26(4), 349-366.

Wagner, B., & Janssen, H. (2022). The EU Artificial Intelligence Act and gender- based harms from deepfakes: Acritical assessment. European Journal of Risk Regulation, 13(2), 302-319.

Whitten, S. (2023). Criminalizing deepfake sexual abuse in the United Kingdom: The need for a specific offence. Criminal Law Review, 2023(4), 281-297.

Wittes, B., Quirk, C., & Lerner, J. (2021). Deepfake detection and platform responsibility. Bookings Institution.

Zheng, Y., & Lee, M. K. (2024). Victim- centric design of deepfake reporting systems: Insights from survivors. Proceedings of the ACM on Human- Computer Interaction, 8(CSCW1), Article 112.