The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2025

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

THE LEGAL VACUUM IN REGULATING NON-CONSENSUAL AI-GENERATED PORNOGRAPHY IN INDIA

Subha Venkatraman

ABSTRACT

The rise in AI-enabled non-consensual pornography, commonly referred to as "deepfake pornography," poses significant challenges to modern legal frameworks around the globe. In India, where current laws are insufficient to address this growing issue, victims who primarily are women continue to suffer severe emotional, psychological, and reputational harm. Personal privacy, dignity, and personal autonomy are infringed upon by non-consensual intimate image abuse, particularly when deepfakes are used. However, the current legal system does not implement proper penalties or preventive measures. This paper examines the regulatory gap that allows AI-generated pornography to spread, evaluating the effectiveness of the Information Technology Act, the Indian Penal Code, and the recently enacted Digital Personal Data Protection Act, 2023. While each statutory instrument addresses certain cybercrimes, none articulates unequivocal prohibitions against deepfake material, and the absence of a discrete statute prohibiting the manufacture and circulation of non-consensual AI-generated pornography further undermines the protection of victims.[1]

The Indian Penal Code includes provisions such as Section 354, which penalises outraging the modesty of a woman, and Section 500, which criminalises defamation, yet their relevance to AI-generated sexualised images remains too general to afford victims consistent protection. Similarly, the Information Technology Act, 2000, contains sections like 66E (violation of privacy), 66D (cheating by personation), and 67 (publishing obscene material), but falters in addressing the novel techniques of synthetic media production. The Indian Cyber Crime Coordination Centre and recent Meta Oversight Board proceedings document

[1] Vittoria Elliott, Celebrity Deepfake Porn Cases Will Be Investigated by Meta Oversight Board, Wired (Apr. 16, 2024), https://www.wired.com/story/meta-oversight-board-deepfake-porn-facebook-instagram/

how the content moderation protocols of platforms such as Facebook and Instagram have been reactive rather than anticipatory, resulting in the slow extraction of harmful material and leaving affected individuals exposed.[2] The delayed removal of deepfake pornography targeting Indian public figures underscores this inadequacy; repeated notifications to the platforms did not deter the further spread of the material, as confirmed by a Reuters report of 2024. Such lapses reveal an urgent gap between the statutory framework and emerging technological realities of harm.[3]

This study contends that the absence of tailored statutory safeguards in India renders individuals especially vulnerable to the harms of deepfake pornography, necessitating prompt legislative redress. Through a comparative examination of jurisdictions like the United States, United Kingdom, and Australia which have progressively enacted prohibitions on the manufacture and dissemination of non-consensual synthetic sexual imagery the study articulates a prospective Indian legal architecture. Central to the design is the introduction of a discrete statutory offense criminalizing the production and circulation of such fabrications absent affirmative, prior consent, accompanied by graduated custodial and pecuniary sanctions. The framework is predicated on a consent-oriented paradigm, stipulating that any likeness deployed in AI-mimetic sexual content must rest on antecedently secured, unequivocal authorization. Furthermore, the analysis recommends an integration of synthetic pornography within the identity misappropriation stipulations of the Information Technology Act, thereby extending the purview of Section 66C to unequivocally encompass the unauthorized appropriation of digital likenesses enabled by generative algorithms.

This study further examines how innovations in detection technology including platforms like Vastav.AI can be augmented by collaborative frameworks joining law enforcement, service providers, and forensic specialists to strengthen both identification and legal redress. Alongside these measures, the analysis highlights the imperative of developing victim-oriented support structures, encompassing streamlined content removal protocols, restitution mechanisms, and psychological services, which together form essential pillars of an effective regulatory matrix. Ultimately, the investigation indicates that, in order to shield

[2] Saumya Ranjan Dixit, Countering Non-Consensual Deepfakes: Proposing a Legal Solution, L. Sch. Pol'y Rev. (Aug. 18, 2024), https://lawschoolpolicyreview.com/2024/08/18/countering-non-consensual-deepfakes-proposing-a-legal-solution/

[3] Reuters, Meta Oversight Board Tells Company to Clean Up Rules on AI-Generated Pornography, Reuters (July 25, 2024), https://www.reuters.com/technology/artificial-intelligence/meta-oversight-board-tells-company-clean-up-rules-ai-generated-pornography-2024-07-25/

individuals from the pervasive dangers of AI-mediated non-consensual pornography, India must institute an all-inclusive legislative framework.

INTRODUCTION

The rapid integration of artificial intelligence across diverse sectors has undeniably yielded transformative gains. Yet, its deployment in the generation of non-consensual pornography, notably through deepfake algorithms, constitutes a profound assault on the triadic values of privacy, dignity, and bodily autonomy. Deepfake pornography is defined as the synthetic fabrication of audiovisual material in which an individual's face and, in some instances, voice, are algorithmically superimposed onto explicit scenarios without the subject's approval. Initially a derivative of non-consensual intimate imagery, the technique's refinement in meticulously reproducing facial geometries and vocal timbres has magnified the reputational and psychological injury inflicted on victims. Within the Indian legal context, the absence of tailored statutes governing the production and distribution of such non-consensual, AI-mediated representations has consigned affected individuals to a punitive limbo, revealing a legislative void that demands immediate and precise redress.[4]

Current legal frameworks in India, including the Indian Penal Code, 1860, and the Information Technology Act, 2000, seek to curtail various cybercrimes, yet they inadequately engage with the specific challenges posed by AI-generated content. Under the IT Act, Section 66E prohibits interference with privacy by the unconsented use of an actual image, yet it remains silent on instances in which a likeness is entirely synthesized. Similarly, Section 67 outlaws the circulation of obscene material, but it is deficient in cases of deepfake pornography since it does not differentiate between the illicit image itself and the algorithmic processes that facilitate its creation and dissemination. Such legal inadequacies expose individuals' women in particular to an escalating spectrum of digital abuse that inflicts profound emotional, psychological, and social injury. Victims frequently endure reputational decay, chronic emotional turmoil, and a disorienting disavowal of bodily autonomy, as manipulated likenesses are weaponized to realise distinct, malicious ends.[5]

---

[4] Anuradha Chakraborty & Sanyogita Tiwari, An Analytical Study on Challenges and Gaps in India's Cyber Security Framework, Int'l J. Crim., Common & Statutory L. (Vol 5, Iss 1, 2025), 4–7, 20. https://doi.org/10.22271/27899497.2025.v5.i1a.110

[5] Mahrus Ali et al., Deepfakes and Victimology: Exploring the Impact of Digital Manipulation on Victims, 8 Substantive Just. Int'l J.L. 1 (2025), https://doi.org/10.56087/substantivejustice.v8i1.306

The enacted Digital Personal Data Protection Act, 2023, while a significant step for data privacy, offers civil but not criminal remedies. It fails to offer definitive measures against the creation and circulation of AI-generated pornography.[6] The absence of promptly enacted criminal safeguards has placed substantial strain on platforms like Facebook and Instagram in moderating user-uploaded content. The Meta Oversight Board recently considered incidents involving Indian public figures whose likenesses were manipulated in deepfake pornography and distributed across its platforms.[7] Although Meta has committed resources to remove the offending material, the absence of an automated detection mechanism has produced a lag in response times and a patchy execution of content governance.

Recent international initiatives from jurisdictions such as the United States, United Kingdom, and Australia reveal several approaches to outlaw the production and dissemination of deepfake pornography without user consent. In the U.S., the proposed DEFIANCE Act of 2024 empowers individuals whose likenesses have been manipulated to initiate civil suits against producers and distributors of such material.[8] In parallel, the United Kingdom has enacted the Online Safety Act 2023, which renders the sharing of non-consensual deepfake pornography a specific crime.[9] Collectively, these transnational legal instruments may inform Indian lawmakers as they contemplate measures to shield citizens from the psychosocial and reputational injuries associated with AI-assisted sexual exploitation.

India presently lacks a systematic and enforceable legal structure that adequately addresses the proliferation of AI-generated non-consensual pornography, resulting in considerable ambiguity for individuals and for service platforms alike. To constrain the injury this phenomenon inflicts, it is incumbent upon the Indian legislature to formulate statutes that categorically prohibit the generation, retention, and dissemination of non-consensual material produced through artificial intelligence. Complementary provisions must, at a minimum, articulate a precise legal conception of consent, delineate sufficient remedial pathways for affected parties, and impose conditional liability upon intermediary platforms for the material

---

[6] The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), Gazette of India, Extraordinary, Part II, Section I (Aug. 11, 2023), https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

[7] Kartik Sharma, Tackling the Deepfake Menace: The Dark Side of AI, Times of India (AI Musings Blog) (Mar. 1, 2024, 4:16 PM), https://timesofindia.indiatimes.com/blogs/ai-musings/tackling-the-deepfake-menace-the-dark-side-of-ai/

[8] Disrupt Explicit Forged Images and Non-Consensual Edits Act of 2024, S. 3696, 118th Cong. (2023–2024), https://www.congress.gov/bill/118th-congress/senate-bill/3696/text

[9] Online Safety Act 2023, c. 50 (UK), enacted Oct. 26, 2023, https://www.legislation.gov.uk/ukpga/2023/50

they store and distribute. Absent the introduction of such comprehensive legal instruments, India will likely persist as a particularly permissive environment for digital abuse and for gender-based violence manifested through AI-facilitated pornography.

LEGAL LANDSCAPE IN INDIA

In India, the regulatory framework directed at non-consensual AI-generated pornography has yet to coalesce into an adequate protective mechanism, exposing victims to an expanding wave of digital coercion. Present legislative instruments, notably the Indian Penal Code, 1860, and the Information Technology Act, 2000, do engage with digital privacy, defamation, and obscenity offences, yet they manifest a critical lack of granularity regarding AI-produced manifestations.[10]

The Indian Penal Code contains certain provisions that, in theory, might be extrapolated to non-consensual deepfake pornography; yet, these provisions lack the specificity required. Section 354, which penalizes the exertion of force against a woman aimed at outraging her modesty, might be invoked, but the text does not expressly contemplate the use of AI to fabricate intimate imagery.[11] Section 500, concerning defamation, could be engaged when a victim's esteem is injured; yet, the clause remains indifferent to the covert digital tampering involved. Consequently, their inability to accommodate the complexities of AI-mediated content leaves significant lacunae in the penal framework.

The Information Technology Act was designed to manage cybercrime, yet its mechanisms present significant deficiencies. While Section 66E prohibits the unauthorized capture or dissemination of private images, it constrains its focus to the physical act of imaging, thereby excluding products of generative AI.[12] Section 66D, which penalises impersonation through identity theft, might on a conceptual level extend to deepfake pornography, yet judicial application is absent. Concurrently, Section 67, which outlaws the electronic publication of obscene material, could account for the distribution of generative pornography, although its application to synthetic media remains unsettled by courts.

---

[10] Anuradha Chakraborty & Sanyogita Tiwari, An Analytical Study on Challenges and Gaps in India's Cyber Security Framework, Int'l J. Criminal, Common & Statutory Law (Vol. 5, Issue 1, 2025) 4-7, DOI: 10.22271/27899497.2025.v5.i1a.110, https://www.criminallawjournal.org/article/110/5-1-3-412.pdf

[11] The Indian Penal Code, 1860, Act No. 45 of 1860 (India), http://dspace.lpu.in:8080/jspui/bitstream/123456789/6183/1/NS%20THESIS%20FINAL%20100_%2004%20%20SEP%202024%20NH.pdf (last accessed Jul. 28, 2025)

[12] The Information Technology Act, 2000, Act No. 21 of 2000 (India), https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (last accessed Jul. 28, 2025)

The recently enacted Digital Personal Data Protection Act, 2023 (DPDP Act) offers a new, albeit incomplete, avenue for redress. Under the DPDP Act, an individual's image or likeness qualifies as "personal data." The creation of a deepfake using this data without explicit, informed, and freely given consent constitutes a breach of the Act.[13] This would make the creator and, in some cases, the distributing platform ("Data Fiduciaries") liable for significant financial penalties. However, the DPDP Act is a civil law; it does not criminalize the act itself, nor does it provide for imprisonment or other penal consequences, which are essential for deterrence in cases of severe abuse.

One primary obstacle to regulating non-consensual deepfake pornography in India lies in the combined complexities of detection and attribution. Generative adversarial networks (GANs) produce outputs indistinguishable from authentic recordings. This makes it difficult for victims to prove a fabrication and for investigators to trace perpetrators. Although detection solutions such as the tool Vastav.AI have been designed to flag deepfakes, their application within India remains sporadic and limited.[14]

Ultimately, while India possesses an array of statutory instruments that could be deployed against non-consensual pornography produced through AI, these instruments fall short of a comprehensive regulatory architecture. The substantive criminal provisions of the IPC and IT Act prove inadequate. As the underlying technologies progress, the Indian legislative assemblage must be recalibrated to incorporate more precisely calibrated legal norms that not only criminalise the origination and transmission of non-consensual deepfake pornography but also articulate unambiguous reparative pathways for aggrieved parties.

COMPARATIVE LAW: GLOBAL RESPONSES

The proliferation of non-consensual, AI-generated pornography has provoked widespread alarm, prompting several nations to address lacunae in their legal architectures. While India's statutory infrastructure remains inchoate, the United States, United Kingdom, Australia, and South Korea have advanced legislative packages to contain this phenomenon. This study systemically contrasts their responses to distil principled features that India might borrow.

---

[13] The Digital Personal Data Protection Act, 2023, Act No. 22 of 2023 (India), https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last accessed Jul. 28, 2025)

[14] India Launches Vastav AI: A Breakthrough in Deepfake Detection Technology, Infopercept (Apr. 12, 2025), https://www.infopercept.com/news/deepfake-no-more-vastav-ai-can-detect-ai-generated-photos-and-videos-in-seconds

REGULATORY ENVIRONMENT IN THE UNITED STATES

In the United States, regulation has evolved through federal and state initiatives. At the federal level, the proposed Disrupt Explicit Forged Images and Non-Consensual Edits Act of 2024 **(DEFIANCE Act)** would create a federal civil right of action for victims of digital forgeries. It allows individuals to sue for damages against those who knowingly produce, distribute, or solicit non-consensual deepfakes. On the state level, California enacted a law in 2020 that outlaws the creation of sexually explicit deepfakes absent the subject's consent, establishing a robust model of state intervention. However, this fragmented approach creates jurisdictional challenges, and First Amendment considerations regarding free expression continue to complicate the drafting of comprehensive prohibitions.[15]

UNITED KINGDOM

The United Kingdom has adopted one of the most direct approaches through its **Online Safety Act 2023**. This landmark legislation created new criminal offenses specifically targeting intimate image abuse. Section 188 of the Act criminalizes the sharing of an "intimate photograph or film," and importantly, the definition includes images that "appear to show" a person in an intimate state, thereby explicitly covering deepfakes.[16] The law makes it an offense to share such material without consent, even if there was no intent to cause distress. This focus on the lack of consent, rather than the perpetrator's motive, is a critical development. Furthermore, the Act imposes proactive duties on online platforms to identify and remove such illegal content.

AUSTRALIA

Australia strengthened its legislative framework with the **Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Act 2018**. This statute amends the Criminal Code Act 1995 to introduce criminal offenses and civil penalties for posting or threatening to post intimate images without consent. The law explicitly includes digitally altered images, covering deepfakes.[17] It prescribes penalties of up to three years of imprisonment, focusing

---

[15] TP James, Not Her Fault: AI Deepfakes, Nonconsensual Pornography, and the Burden of Proof, 2025 BYU L. Rev. 1 (2025), https://digitalcommons.law.byu.edu/cgi/viewcontent.cgi?article=3564&context=lawreview

[16] Humzah Ilyas, What Are the New Offences Under the Online Safety Act 2023 (June 10, 2024), Hickman & Rose, https://www.hickmanandrose.co.uk/what-are-the-new-offences-under-the-online-safety-act-2023/

[17] Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Bill 2018, S 1113, 45th Parl., 1st Sess. (Cth) (Austl.), https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1113

on the victim's lack of consent and the perpetrator's culpability. However, as in other jurisdictions, authentication and enforcement remain persistent obstacles.

SOUTH KOREA

South Korea, which has faced a severe deepfake crisis, amended its Act on Special Cases Concerning the Punishment of Sexual Crimes to categorically criminalize the manufacture and circulation of deepfake pornography. The law imposes custodial sentences of up to five years for anyone who generates or disseminates deepfake pornography without the explicit consent of the depicted person. Following a public outcry over digital sex crime rings, the law was further amended to criminalize even the viewing and possession of such material.[24] This robust approach, which combines harsh penalties with rapid takedown mandates for platforms, is often cited as a model for victim-centric deterrence.

These international frameworks furnish instructive precedents, but each exhibits discernible shortcomings related to the transnational character of the internet and the difficulty of content moderation at scale. Nonetheless, the clear trend is toward creating specific criminal prohibitions targeting both the creation and distribution of this material.[18]

CASE STUDIES

The emergence of non-consensual, AI-generated pornography has provoked a series of prominent incidents that illuminate the vulnerabilities of individuals and the deficiencies of existing legal structures.

A salient illustration is the episode involving an Indian actress whose likeness was surreptitiously altered and disseminated in a deepfake pornography campaign. The incident attracted extensive media scrutiny when her image was deployed in sexually explicit materials circulated via Facebook and Instagram. She initiated a formal grievance with the Meta Oversight Board, seeking expeditious removal. Nonetheless, the images persisted online for days, and the platform's response was criticized for its latency. The episode highlights a pronounced lacuna in the Indian statutory apparatus, which lacks the specificity necessary to counter AI-forged pornography.

---

[18] Valerie Maria Johnson, Deepfake Violence and the Future of Human Rights: A South Korean Case Study (Master's thesis, Lund Univ. 2025), LUP Student Papers, record no. 9201985, http://lup.lub.lu.se/student-papers/record/9201985

The United States witnessed a prominent early episode when explicit videos of actress Scarlett Johansson were disseminated with her likeness digitally overlaid. Her public outcry became a focal point for policy debate, contributing to the momentum for legislative reform in California and at the federal level. The incident underscored an enduring gap in statutory regimes and the pressing need for harmonized enforcement frameworks capable of transcending national borders.

In the United Kingdom, the experience of public figures who discovered synthetic replicas of their likenesses in pornographic material attracted considerable media coverage and highlighted the inadequacies of the existing "revenge pornography" laws, which did not explicitly cover AI-generated content. These cases expedited public and political awareness, ultimately fostering the movement toward the more precisely calibrated offenses now included in the Online Safety Act 2023.

Meta's delayed handling of the Indian actress's complaint, Scarlett Johansson's public advocacy, and the legislative responses in the UK and Australia jointly highlight critical weaknesses in oversight.[19] Foremost among these is an absence of precise, universally accepted definitions of consent as it pertains to AI-generated representations. Accompanying this is the persistent problem of latency in content removal, compounded by cross-border enforcement challenges. These incidents make clear that any future legal architecture must extend beyond mere criminalization to encompass anticipatory detection mechanisms, structured prevention programs, and ongoing support for affected individuals.

CONCLUSION

The proliferation of non-consensual AI-generated pornography poses an urgent challenge to both personal privacy and digital justice. Comparative analyses reveal that existing legal instruments in India remain ill-equipped to capture the distinctive modalities introduced by algorithmic synthesis, perpetuating harm through legal inertia. The cases surveyed underscore a systemic deficit whereby the absence of tailored prohibitions generates fragmented enforcement, protracted delays in content remediation, and a conspicuous shortfall in structural protections for victims.

[19] Channel 4 may have violated Sexual Offences Act with deepfake video of Scarlett Johansson, The Guardian (U.K.), Jan. 31, 2025, https://www.theguardian.com/tv-and-radio/2025/jan/31/channel-4-may-have-violated-sexual-offences-act-with-deepfake-video-of-scarlett-johansson

The Indian Penal Code and the Information Technology Act furnish limited pathways for redress, while the new Digital Personal Data Protection Act, 2023, offers only civil remedies. This legislative vacuum becomes especially concerning as AI capabilities advance. Globally, nations including the United Kingdom, Australia, and South Korea have enacted substantial criminal reforms directed at AI-facilitated pornography, concentrating their statutes on both the production and circulation of these materials. The sanctions attached to such offenses, combined with proactive duties on platforms, provide a clear path forward.

The exigency of an exhaustive legislative architecture in India that criminalises the manufacture, propagation, and possession of non-consensual AI-generated pornography is now paramount. Such a structure ought to embed mechanisms for victim-centred redress, including expedited content removal, victim compensation, and dedicated legal assistance. Concurrently, digital intermediaries must incur clear obligations to excise deleterious content and shield users from online harm, in line with frameworks like the UK's Online Safety Act. Definitions of consent must be recalibrated to accommodate the digital milieu, stipulating that any utilisation of an individual's likeness in AI-generated imagery mandates documented, prior, and informed consent.

The swift proliferation of AI-created deepfake pornography necessitates urgent, harmonized intervention. India, consistent with the obligations and precedents of the global community, must now close the extant legislative chasm and fortify the protective architecture surrounding potential targets of non-consensual, algorithmically generated imagery.

REFERENCES:

1. See generally Saumya Ranjan Dixit, Countering Non-Consensual Deepfakes: Proposing a Legal Solution, L. Sch. Pol'y Rev. (Aug. 18, 2024), https://lawschoolpolicyreview.com/2024/08/18/countering-non-consensual-deepfakes-proposing-a-legal-solution/
2. Vittoria Elliott, Celebrity Deepfake Porn Cases Will Be Investigated by Meta Oversight Board, Wired (Apr. 16, 2024), https://www.wired.com/story/meta-oversight-board-deepfake-porn-facebook-instagram/
3. Meta Oversight Board Tells Company to Clean Up Rules on AI-Generated Pornography, Reuters (July 25, 2024),

https://www.reuters.com/technology/artificial-intelligence/meta-oversight-board-tells-company-clean-up-rules-ai-generated-pornography-2024-07-25/

4. 4. Anuradha Chakraborty & Sanyogita Tiwari, An Analytical Study on Challenges and Gaps in India's Cyber Security Framework, Int'l J. Crim., Common & Statutory L. (Vol 5, Issue 1, 2025), 4–7,
5. https://doi.org/10.22271/27899497.2025.v5.i1a.110
6. Mahrus Ali et al., Deepfakes and Victimology: Exploring the Impact of Digital Manipulation on Victims, 8 Substantive Just. Int'l J.L. 1 (2025), https://doi.org/10.56087/substantivejustice.v8i1.306
7. The Digital Personal Data Protection Act, 2023 (Act No. 22 of 2023), Gazette of India, Extraordinary, Part II, Section I (Aug. 11, 2023), https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf
8. Kartik Sharma, Tackling the Deepfake Menace: The Dark Side of AI, Times of India (AI Musings Blog) (Mar. 1, 2024, 4:16 PM), https://timesofindia.indiatimes.com/blogs/ai-musings/tackling-the-deepfake-menace-the-dark-side-of-ai/
9. Disrupt Explicit Forged Images and Non-Consensual Edits Act of 2024, S. 3696, 118th Cong. (2023–2024), https://www.congress.gov/bill/118th-congress/senate-bill/3696/text
10. Online Safety Act 2023, c. 50 (UK), enacted Oct. 26, 2023, available at https://www.legislation.gov.uk/ukpga/2023/50
11. The Indian Penal Code, 1860, Act No. 45 of 1860 (India), http://dspace.lpu.in:8080/jspui/bitstream/123456789/6183/1/NS%20THESIS%20FINAL%20100_%2004%20%20SEP%202024%20NH.pdf (last accessed Jul. 28, 2025)
12. The Information Technology Act, 2000, Act No. 21 of 2000 (India), https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf (last accessed Jul. 28, 2025)
13. The Digital Personal Data Protection Act, 2023, Act No. 22 of 2023 (India), https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf (last accessed Jul. 28, 2025)
14. India Launches Vastav AI: A Breakthrough in Deepfake Detection Technology, Infopercept (Apr. 12, 2025),

https://www.infopercept.com/news/deepfake-no-more-vastav-ai-can-detect-ai-generated-photos-and-videos-in-seconds

15. TP James, Not Her Fault: AI Deepfakes, Nonconsensual Pornography, and the Burden of Proof, 2025 BYU L. Rev. 1 (2025), https://digitalcommons.law.byu.edu/cgi/viewcontent.cgi?article=3564&context=lawreview
16. Humzah Ilyas, What Are the New Offences Under the Online Safety Act 2023 (June 10, 2024), Hickman & Rose, https://www.hickmanandrose.co.uk/what-are-the-new-offences-under-the-online-safety-act-2023/
17. Enhancing Online Safety (Non-consensual Sharing of Intimate Images) Bill 2018, S 1113, 45th Parl., 1st Sess. (Cth) (Austl.), https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=s1113
18. Valerie Maria Johnson, Deepfake Violence and the Future of Human Rights: A South Korean Case Study (Master's thesis, Lund Univ. 2025), LUP Student Papers, record no. 9201985, http://lup.lub.lu.se/student-papers/record/9201985
19. Channel 4 may have violated Sexual Offences Act with deepfake video of Scarlett Johansson, The Guardian (U.K.), Jan. 31, 2025, https://www.theguardian.com/tv-and-radio/2025/jan/31/channel-4-may-have-violated-sexual-offences-act-with-deepfake-video-of-scarlett-johansson