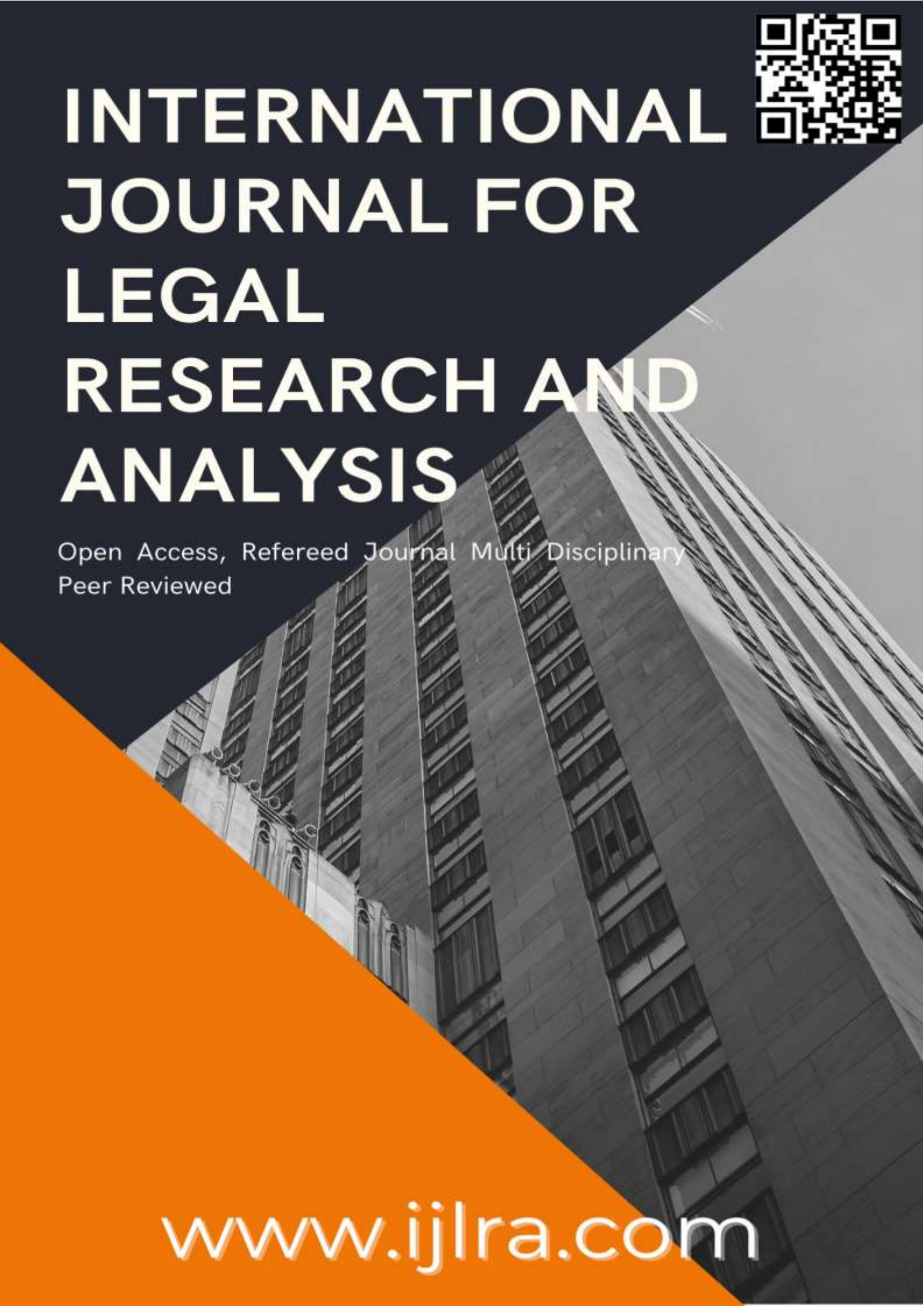
INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed Journal Multi Disciplinary
Peer Reviewed



www.ijlra.com

ISSN: 2582-6433

DISCLAIMER

No part of this publication may be reproduced, stored, transmitted, or distributed in any form or by any means, whether electronic, mechanical, photocopying, recording, or otherwise, without prior written permission of the Managing Editor of the *International Journal for Legal Research & Analysis (IJLRA).*

The views, opinions, interpretations, and conclusions expressed in the articles published in this journal are solely those of the respective authors. They do not necessarily reflect the views of the Editorial Board, Editors, Reviewers, Advisors, or the Publisher of IJLRA.

Although every reasonable effort has been made to ensure the accuracy, authenticity, and proper citation of the content published in this journal, neither the Editorial Board nor IJLRA shall be held liable or responsible, in any manner whatsoever, for any loss, damage, or consequence arising from the use, reliance upon, or interpretation of the information contained in this publication.

The content published herein is intended solely for academic and informational purposes and shall not be construed as legal advice or professional opinion.

ISSN: 2582-6433

ABOUT US

The *International Journal for Legal Research & Analysis (IJLRA)* (ISSN: 2582-6433) is a peer-reviewed, academic, online journal published on a monthly basis. The journal aims to provide a comprehensive and interactive platform for the publication of original and high-quality legal research.

IJLRA publishes Short Articles, Long Articles, Research Papers, Case Comments, Book Reviews, Essays, and interdisciplinary studies in the field of law and allied disciplines. The journal seeks to promote critical analysis and informed discourse on contemporary legal, social, and policy issues.

The primary objective of IJLRA is to enhance academic engagement and scholarly dialogue among law students, researchers, academicians, legal professionals, and members of the Bar and Bench. The journal endeavours to establish itself as a credible and widely cited academic publication through the publication of original, well-researched, and analytically sound contributions.

IJLRA welcomes submissions from all branches of law, provided the work is original, unpublished, and submitted in accordance with the prescribed submission guidelines. All manuscripts are subject to a rigorous peer-review process to ensure academic quality, originality, and relevance.

Through its publications, the *International Journal for Legal Research & Analysis* aspires to contribute meaningfully to legal scholarship and the development of law as an instrument of justice and social progress.

ISSN: 2582-6433

PUBLICATION ETHICS, COPYRIGHT & AUTHOR RESPONSIBILITY STATEMENT

The *International Journal for Legal Research and Analysis (IJLRA)* is committed to upholding the highest standards of publication ethics and academic integrity. All manuscripts submitted to the journal must be original, unpublished, and free from plagiarism, data fabrication, falsification, or any form of unethical research or publication practice. Authors are solely responsible for the accuracy, originality, legality, and ethical compliance of their work and must ensure that all sources are properly cited and that necessary permissions for any third-party copyrighted material have been duly obtained prior to submission. Copyright in all published articles vests with IJLRA, unless otherwise expressly stated, and authors grant the journal the irrevocable right to publish, reproduce, distribute, and archive their work in print and electronic formats. The views and opinions expressed in the articles are those of the authors alone and do not reflect the views of the Editors, Editorial Board, Reviewers, or Publisher. IJLRA shall not be liable for any loss, damage, claim, or legal consequence arising from the use, reliance upon, or interpretation of the content published. By submitting a manuscript, the author(s) agree to fully indemnify and hold harmless the journal, its Editor-in-Chief, Editors, Editorial Board, Reviewers, Advisors, Publisher, and Management against any claims, liabilities, or legal proceedings arising out of plagiarism, copyright infringement, defamation, breach of confidentiality, or violation of third-party rights. The journal reserves the absolute right to reject, withdraw, retract, or remove any manuscript or published article in case of ethical or legal violations, without incurring any liability.

ISSN: 2582-6433

ARTIFICIAL INTELLIGENCE, DIGITAL SAFETY, AND ONLINE GENDER-BASED RISKS: A COMPARATIVE STUDY OF WOMEN'S DIGITAL PARTICIPATION IN INDIA AND THE UNITED STATES

AUTHORED BY - MS SHAHEEN HABIB AND DR DAMINI SAXENA

ABSTRACT

The proliferation of artificial intelligence (AI) tools, social media platforms, and digital communication technologies has created unprecedented opportunities for women's participation in public life while simultaneously generating novel and intensifying forms of gender-based risks in the digital sphere. This paper presents a comparative analysis of the nature, scale, and regulatory responses to online gender-based risks confronting women in India and the United States. Drawing upon Pew Research Center survey data, National Crime Records Bureau (NCRB) reports, UN Women research, parliamentary inquiries, and legislative texts, the paper maps the empirical landscape of technology-facilitated gender-based violence (TFGBV) across both jurisdictions. It examines the evolution of relevant legal frameworks in both countries, including India's Bharatiya Nyaya Sanhita, 2023, the Digital Personal Data Protection Act, 2023 and its Rules 2025, the IT (Intermediary Guidelines) Rules, 2021; and the United States' Violence Against Women Act Reauthorization Act, 2022, the TAKE IT DOWN Act, 2025, and the DEFIANCE Act, and evaluates their effectiveness against the accelerating threat landscape enabled by generative AI, deepfakes, and sextortion. Statistical data is presented in tabular form to facilitate rigorous cross-jurisdictional comparison. The analysis reveals that both countries face a shared crisis of disproportionate digital targeting of women, but differ materially in legislative design, platform accountability mechanisms, and enforcement infrastructure.

Keywords: Deepfakes; Online Harassment; Digital Safety; India; United States; Artificial Intelligence;

ISSN: 2582-6433

INTRODUCTION

The global digital transformation of the last decade has changed the topology of gender-based violence radically. From physical boundaries that previously bound the reaches of harassment, stalking and sexual exploitation, digital networks have removed these barriers to perpetrators targeting women on different continents, with impunity, anonymity and emerging technological sophistication. The development and spread of generative artificial intelligence has increased the qualitative level of this threat further: Deepfake technologies, made possible by AI, now allow non-consensual sexually explicit content creation at scale, with little technical knowledge, target personalized abuse of any woman whose image is publicly available.[1]

The numbers are stark. Furthermore, according to UN Women, 38% of women worldwide have experienced online violence and 85% of online damage have been observed by women.[2] In the United States, a recent 2021 nationally representative Pew Research Center survey found that 38% of women reported experiencing some type of online harassment, 16% specifically reported online sexual harassment.[3] In India, where there are now more than 800 million internet users, the National Crime Records Bureau (NCRB) counted 66,833 cases of cybercrime in 2022 alone, with women heavily in the mix when it comes to being the victim of a violation of their privacy and/or sexual harassment offences. Yet these levels almost certainly underestimate the dimensions of the problem in view of chronic and under-reporting given the stigma in reporting and a lack of digital literacy as the devices are privacyable in nature, among other factors.[4]

TYPOLOGY OF ONLINE GENDER-BASED RISKS AND AI-ENABLED HARMS

Technology-Facilitated Gender-Based Violence: Core Manifestations

Technology-facilitated gender-based violence (TFGBV) is a broad category that covers misuse of digital tools to commit harmful acts against his/her victims because of gender. Its principal manifestations include: Cyberstalking (persistent online surveillance and threatening contact),

[1]United Nations Secretary-General, 'Intensification of Efforts to Eliminate All Forms of Violence Against Women and Girls: Technology-Facilitated Violence Against Women and Girls' (UN Women, New York, 2024).
[2]UN Women, 'AI-Powered Online Abuse: How AI Is Amplifying Violence Against Women and What Can Stop It' (UN Women Headquarters, 2024) <https://www.unwomen.org/en/articles/faqs/ai-powered-online-abuse-how-ai-is-amplifying-violence-against-women-and-what-can-stop-it> accessed 1 March 2026.
[3]Emily A. Vogels, "The State of Online Harassment' (Pew Research Center, 13 January 2021) <https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/> accessed 1 March 2026.
[4]National Crime Records Bureau, Ministry of Home Affairs, 'Crime in India 2022' (NCRB, New Delhi, 2023).

ISSN: 2582-6433

the non-consensual publication of personal identifying information - doxing, non-consensual intimate imagery - NCII, or 'revenge porn', online sexual harassment, image-based abuse, sextortion, impersonation and coordinated harassment campaigns.[5] While anyone can be the target, targeting of women in all these envelopes in disproportionate amount is well-documented. According to the New York State Office for the Prevention of Domestic Violence, "according to research, 66 of women worldwide report that they are the victims of cyber harassment, 55 that they experience doxing, and 63 that they are the victims of hacking and stalking.'

Among these, NCII defined as the distribution of sexually explicit imagery of a person without his or her consent is one of the most psychologically devastating. Studies find that, of NCII victims, 93% suffer significant emotional distress, 90% of all NCII victims reported are women.[6] Feminine username on online platforms produce as much as 25 times the amount of gendered targeted abuse suggesting that there is a structural misogyny built into how women's experience online.

Artificial Intelligence as a Force Multiplier for Gender-Based Online Harm

The wave of democratization of generative AI arrival has fundamentally changed the threat landscape for women online. Deepfake technology which harnesses the power of machine learning to trace out fabricated images, sound and video has emerged to be the main vehicle in AI-enabled sexual abuse. The total number of deepfake videos in the world in 2023, is 550% greater than in 2019 and deepfake pornography accounts for 98% of all deepfake pornography and 99% of the people shown in non-concensual deepfake pornography are women.[7] The number of such videos has increased nine-fold since 2019 and have been viewed almost four billion times globally.[8]

Beyond deepfakes, AI makes possible sophisticated doxing campaigns, AI-driven catfishing so that people can be sextorted, and the automated massive scaling of coordinated harassment. Natural language processing tools can detect vulnerable or sensitive content posted about women in public spaces, which makes it easier for them to be targeted for harassment on an organized basis. As UN Women has seen, many deepfake tools are structurally gendered: they

[5]Office of the Prevention of Domestic Violence, New York, 'Technology-Facilitated Gender-Based Violence' (OPDV, 2024) <https://opdv.ny.gov/technology-facilitated-gender-based-violence> (citing global data: 66% of women report experiencing cyber harassment; 55% report doxing; 63% report hacking and stalking).
[6]Women's Media Center, 'Research & Statistics on Online Harassment' (Women's Media Center, 2024) <https://womensmediacenter.com/speech-project/research-statistics> accessed 1 March 2026.
[7]UN Women (n 2).
[8]Laffier J and Rehman A, 'Deepfake Statistical Data (2023-2025)' (2023).

ISSN: 2582-6433

are often designed to work only on female bodies, with nudifier and face-swap applications not working on images of male bodies owing to the design biases of primarily male development teams.[9]

COMPARATIVE STATISTICAL OVERVIEW

The following tables present empirical data on the incidence of online gender-based risks and the comparative regulatory landscape across India and the United States.

Table 1: Comparative Statistics on Online Gender-Based Violence – India and the United States

Indicator	India	United States
Women experiencing online harassment (self-reported)	~59% of women reported digital/gender-based harassment (NFHS-5 / ICT-facilitated GBV data)	38% of women report any form of online harassment; 16% report online sexual harassment (Pew Research, 2021)
Young women (18–35) facing online sexual harassment	No disaggregated national data; high incidence reported in urban cybercrime cells	33% of women under 35 report online sexual harassment (Pew Research, 2021)
Deepfake pornography victims (% female)	99% of deepfake porn targets are women globally; India reported cases rising rapidly (UN Women, 2024)	99% of deepfake pornographic content targets women; nonconsensual deepfake videos up 550% from 2019 to 2023 (UN Women, 2024)
Women parliamentarians facing online violence	76% in Asia-Pacific experience psychological violence online (IPU, 2024)	25 of 26 Congress members depicted in nonconsensual imagery were women (American Sunlight Project, 2024)
Online cyberstalking	Women disproportionately	Women 13% vs. men 9%

[9]UN Women (n 1).

ISSN: 2582-6433

(gender gap)	targeted; 37% of cybercrime cases involve women (NCRB 2022)	stalked online; women 3x more likely to cite gender as motive (Pew, 2021)
Reported cybercrimes against women (latest year)	66,833 cybercrime cases reported (NCRB 2022); significant under-reporting suspected	FTC received 1.1 million reports of identity theft and cybercrime in 2023; gendered data not fully disaggregated
Women self-censoring/withdrawing from online activity	Significant self-censorship documented especially among journalists and public figures	27% of women harassed online modified their online behavior; 11% temporarily stopped use (Pew, 2021)

Sources: Pew Research Center (2021); UN Women (2024); NCRB Crime in India Report (2022); Inter-Parliamentary Union (2024); American Sunlight Project (2024); Newsweek/Incogni (2026).

Table 1 shows some critical patterns. First, the Pew data from the United States offers a degree of disaggregation by gender and age that Indian governmental data does not have the granular understanding of who is being harassed and how, which is a necessary prerequisite for evidence-based legal reform. Second, the deepfake phenomena are a global phenomenon that is overwhelmingly directed at women and whose challenges demand international coherent regulatory responses, rather than merely domestic responses. Third, the pattern of self-censorship and behavioural withdrawal the harassed could not instill in themselves as reported by 27% of women in the US almost certainly underestimates that in India where a culture of social stigma and institutional distrust further deter open participation in digital communities.[10]

Table 2: Comparative Legal and Regulatory Framework – India and the United States

Legal Instrument	India	United States
Primary online safety law	Information Technology Act, 2000 (as amended 2008);	Violence Against Women Act Reauthorization Act, 2022 (P.L.

[10]Paige Leskin and others, 'Online Harassment Isn't Growing But It's Getting More Severe' (Pew Charitable Trusts, 28 June 2021) <https://www.pew.org/en/trust/archive/spring-2021/online-harassment-isnt-growing-but-its-getting-more-severe> accessed 1 March 2026.

ISSN: 2582-6433

	Sections 66E, 67, 67A	117-103); Title XIV on Cybercrimes
Stalking provision	Bharatiya Nyaya Sanhita, 2023, § 78 (cyberstalking, up to 3–5 years imprisonment)	18 U.S.C. § 2261A (federal cyberstalking); VAWA 2022 strengthened enforcement
Non-consensual intimate images (NCII)	No dedicated NCII law; reliance on IT Act § 66E (privacy violation, up to 3 years imprisonment)	TAKE IT DOWN Act (signed May 19, 2025); VAWA 2022 civil cause of action for NCII
AI-generated deepfakes (nonconsensual)	No specific deepfake legislation; prosecuted under IT Act § 66E/67/67A and BNS provisions	TAKE IT DOWN Act, 2025; DEFIANCE Act (Senate-passed July 2024; reintroduced May 2025) provides civil right of action
Data protection and online privacy	Digital Personal Data Protection Act, 2023; DPDP Rules, 2025 (notified November 13, 2025)	No comprehensive federal data privacy law; state-level (California CPRA, etc.); FTC enforcement authority
Platform accountability / intermediary rules	IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (amended 2023)	Section 230 of CDA, 1996; nascent platform accountability proposals under debate (2024–2025)
Penalty range	IT Act § 67A: up to 7 years imprisonment and ₹10 lakh fine for sexually explicit content	TAKE IT DOWN Act: civil penalties; VAWA 2022 Title XIV: federal criminal provisions with imprisonment

Sources: IT Act, 2000; Bharatiya Nyaya Sanhita, 2023; DPDP Act, 2023; IT Rules, 2021; VAWA 2022 (P.L. 117-103); TAKE IT DOWN Act, 2025; DEFIANCE Act, S.3696 (2024).

ISSN: 2582-6433

INDIA'S LEGAL FRAMEWORK: ARCHITECTURE AND GAPS

The Information Technology Act, 2000 and the BNS, 2023

The main primary of India's response to technology-facilitated gender-based violence as a statutory response is scattered across three overlapping instruments. Most directly relevant provisions are contained in The Information Technology Act, 2000. Section 66E deals with the offence of capturing, publishing or transmitting private images without consent and is punishable by imprisonment for a period up to three years or by a fine of up to Rs. two lakh.[11] Sections 67 and 67A deal with obscene and sexually explicit material online, and Section 67A has penalties ten times harsher punishable up to five years in prison for a first-time offence. However, these provisions existed before generative AI by almost a decade, and the Supreme Court striking down of Section 66A in Shreya Singhal vs the State of Himachal Pradesh, Supplementary Application of Communications and Information Networks v The State of Himachal Pradesh. union of india (2015) removed one channel of redress of offensive online content, there remains a legislative gap.[12]

The Bharatiya Nyaya Sanhita, 2023, which is being applied instead of Indian Penal Code date 1st July 2024 is momentous move towards modernization of Indian Criminal-mo Criminal law. Section 78 of the BNS specifically punishes cyberstalking with imprisonment of three years for the first offence and five years for subsequent offences.[13] Sections 76 and 77 address online sexual harassment and digital voyeurism respectively.[14] Despite all these advances, the BNS fails to cover AI-generated deepfakes and NCII as separate categories of crimes requiring prosecutors to turn to analogical application of existing provisions which creates a significant structural deficiency in light of the magnitude of the deepfake crisis.

The Digital Personal Data Protection Act, 2023 and DPDP Rules, 2025

The Cybercrime and Data Privacy Convention of India The Digital Personal Data Protection Act, 2023 (DPDP Act) is India's most important chapter in the digital rights law of late. Enacted on August 11, 2023 and operative with effect from October 27, 2025 through the notification of the rules by the Ministry of Electronics and Information Technology, Dept. of Electronics and Information Technology (DPDP Rules) dated January 6, 2023 notified by the Ministry of Electronics and Information Technology, notification date - Nov 13 2023, the same

[11]Information Technology Act, 2000, No. 21 of 2000, Acts of Parliament, 2000 (India) [hereinafter IT Act], § 66E.
[12]Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[13]Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, Acts of Parliament, 2023 (India) [hereinafter BNS], § 78.
[14]BNS, § 76 (sexual harassment including online) and § 77 (voyeurism including digital); see also IT Act, § 66E.

ISSN: 2582-6433

gives a comprehensive basis for processing of digital personal data, constitute organisation known as Data Protection Board of India, and prescribes the punishments for breaching the data Critically also, these principles of data minimization, purpose limitation, and storage limitation need to be strongly enforced, and have real-world potential to significantly limit the ability of platforms to facilitate the aggregation and weaponization of personal data for doxing and identity theft targeting women. The Act is also significant since it is the first Indian legislation to use 'she/her' pronouns, which is an explicit commitment to gender-inclusivity.

The IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (as amended in 2023) place certain obligations on the significant social media intermediaries to have a Grievance Officer in India, to acknowledge the complaints related to NCII and sexual harassment within 24 hours, and resolve such complaints within 15 days. However, the provision in the Rules that obliges intermediaries to facilitate identification of the originator of encrypted communications on request by the government has been widely criticized by civil society as a threat to privacy and encrypted communication that may have a paradoxical effect of discouraging women from using secure channels to report harassment.[15]

Structural Gaps in India's Framework

Notwithstanding these legislative developments, India's regulatory framework for ensuring digital safety for women does contain large structural gaps. Most significantly, India does not have any separate law on NCII or deepfakes generated with AI. The protection of privacy enshrined in the constitution in K.S. Puttaswamy v. Union of India (2017)[16] provides a constitutional basis of digital privacy rights at a fundamental level, yet the gap between the constitutional principle and effective protection in law is still great; There is not a civil right of action created equivalent to the one created by VAWA 2022 in the United States. Enforcement is much reliant on police lodging FIRs being a process that generates well-documented barriers for women, including victim blaming attitudes, lack of technical expertise, and geographic inaccessibility.[17]

[15]IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, Rule 4(1)(b).
[16]K.S. Puttaswamy v. Union of India, (2017) 10 SCC 1.
[17]Human Rights Watch, '#MeToo in India: Poor Enforcement of India's Sexual Harassment Law' (HRW, 2020); SabrangIndia (n 6).

ISSN: 2582-6433

THE UNITED STATES' LEGAL FRAMEWORK: ADVANCES AND ONGOING CHALLENGES

VAWA 2022 and the Expansion of Cybercrime Protections

The latest attempt to tackle technology-driven gender-based violence at the federal level is the Violence Against Women Act Reauthorization Act of 2022 (P.L. 117-103), which was signed by President Biden on March 15, 2022. Title XIV of VAWA 2022 specifically addresses cybercrimes against individuals, creating new grant programs for state, tribal and local law enforcement to address cyberstalking, sextortion and online harassment, and directs the Attorney General to develop a national strategy on cybercrimes against individuals. VAWA 2022 also established a federal civil cause of action pertaining to the non-consensual disclosure of intimate images that will allow survivors to seek damages from and injunctive relief against others while allowing them to maintain anonymity through the use of a pseudonym. Between 1993 and 2022, domestic violence rates have decreased by 67% and sexual assault rates by 56%, showing the impact of the cumulative effort of VAWA, which has been investing now for 30 years.[18]

The TAKE IT DOWN Act, 2025 and the DEFIANCE Act

The most recent and direct legislative response to AI-enabled gender-based online violence in the United States is the TAKE IT DOWN Act, signed into law by President Trump on May 19, 2025.[19] The Act results in social media platforms and websites having to create processes for the removal of non-consensual intimate imagery both real and AI generated within 48 hours of a verified report. Platforms that don't do so are subject to civil and criminal penalties, and creators and distributors of such content are guilty of a federal crime. By 32 states having already passed similar legislation before the federal legislation, the Act codifies and replaces the patchwork of protections at the state level. The DEFIANCE Act Disrupt Explicit Forged Images and Non-Consensual Edits Act was passed by the United States Senate without dissent on July 23, 2024 which created a federal civil right-of-action for people who knowingly produce, distribute, solicit, or receive non-consensual sexually explicit deepfakes.[20] The Act

[18]National Center on Domestic and Sexual Violence, 'Violence Against Women Act: 30th Anniversary' (NCDSV, September 2024) <https://www.ncdsv.org/violence-against-women-act-vawa-30th-anniversary-september-2024.html> accessed 1 March 2026.

[19]Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks Act (TAKE IT DOWN Act), Pub. L. No. 119-___ (signed May 19, 2025).

[20]U.S. Senate Judiciary Committee, 'Durbin Applauds Senate Passage of His Bipartisan Bill to Tackle Nonconsensual, Sexually-Explicit Deepfakes' (Press Release, July 23, 2024) <https://www.judiciary.senate.gov/press/dem/releases/durbin-applauds-senate-passage-of-his-bipartisan-bill-to-

ISSN: 2582-6433

was reintroduced in 119th Congress in May 2025 in conjunction with the passage of TAKE IT DOWN as the dual legislative approach of combining efforts of TAKE IT DOWN on platform-level removal obligations and criminal liability and the DEFIANCE Act, which is intended to empower individual survivors with civil remedies against their perpetrators.[21] The Act provides for liquidated damages of $150,000 (or $250,000 in aggravated circumstances), a ten-year statute of limitations, and does not pre-empt more protective state laws.[22]

Limitations of the US Framework

Notwithstanding these advancements, the United States' regulatory model with regards to women's digital safety has some notable weaknesses. The lack of a comprehensive federal data privacy law as opposed to the DPDP Act 2023 in India and the European GDPR, there is a gap that permits critical information about women and the aggregation of that information for doxing to identity-based harassment.[23] Section 230 of the Communications Decency Act of 1996, which grants immunity to platforms for user content, has protected the platforms from liability for content of harassment. The TAKE IT DOWN Act achieves a specific carve-out to this immunity, but more extensive protections to make platforms accountable is subject to some debate. Further, the fact that the 25% of women surveyed in 2026 who experienced online abuse rose to 27% and the particularly vulnerable nature of both publicly revealable populations of women - namely the trans group" (LGBTQ+) and progressing women of colour (non-white) - this makes it appear that existing protections are inadequate for the most marginalised.[24]

COMPARATIVE ANALYSIS AND RECOMMENDATIONS

Convergences and Divergences

The comparative analysis discloses that there are both convergences as well as material divergences between the two jurisdictions. However, the concept of TFGBV has already been

tackle-nonconsensual-sexually-explicit-deepfakes> accessed 1 March 2026.

[21]Disrupt Explicit Forged Images and Non-Consensual Edits Act (DEFIANCE Act), S. 3696, 118th Cong. (2024).

[22]Representative Alexandria Ocasio-Cortez, Press Release: 'Ocasio-Cortez, Lee, Durbin, Graham Introduce Bipartisan, Bicameral Legislation to Combat Non-Consensual, Sexually Explicit Deepfake Imagery' (May 21, 2025) <https://ocasio-cortez.house.gov/media/press-releases/ocasio-cortez-lee-durbin-graham-introduce-bipartisan-bicameral-legislation>.

[23]Sandra Wachter (Professor of Technology and Regulation, Oxford Internet Institute), quoted in Newsweek ibid ('Unless legislators (and society) start to treat these offenses more seriously, tech will be weaponized against women').

[24]Newsweek, 'Women Are Facing Growing Online Abuse' (Newsweek, 6 March 2026) <https://www.newsweek.com/women-online-abuse-rising-study-trump-administration-ai-11624655> accessed 6 March 2026.

ISSN: 2582-6433

identified in both India and the United States as a significant societal issue that is to be addressed by means of specific law. In 2022-2025, both jurisdictions have taken a step forward in their legislative programs to include non-consensual intimate imagery and AI-generated deepfakes. Both too have noted that platform-level regulation in the form of intermediary obligations and content removals is a required parameter in and above individual criminal or civil responsibility.

The points of difference are however high. The United States has created a more advanced and person-focused civil remedy framework, such as the civil right of action with adverse liquidated damages in the DEFIANCE Act, whereas India is forming more on criminal cases that women can barely afford. In India, it has taken a pace in regard to all-encompassing data protection with the framework of the DPDP Act 2023 and the Rules 2025, which at the federal level the United States still does not have. The intermediary regulations of India have stricter and quicker response deadlines on the platform compared to the current laws in the US, involving federal procedures, but they are not always enforced. More importantly, India has not yet established specific NCII or deepfake statutes and courts and prosecutors rely on analogical reasoning during the IT Act and BNS process, which simply does not work regarding the rapidity and scope of AI-based damage.[25]

Recommendations

Wholesine recommendations are made, based on this comparative examination, in both jurisdictions as follows:

To start with, India must immediately pass specific NCII and AI deepfake laws based on the TAKE IT DOWN Act, including both a criminal offense of creating and distributing AI-generated intimate imagery non-consensually and a civil remedy of action category on the survivors who could have sustained significant damages. Present dependency on analogical application of the IT Act and the BNS is not appropriate structurally in the current rate of technological changes.

Second, India and United States must require data collection, though gender-disaggregated and platform-specific, on Internet-based harassment cases that people report and get taken down to allow introducing evidence-based policies and holding platforms responsible on the unequal effects of their products on women.

[25]Government of United Kingdom, Home Office, 'Country Policy and Information Note: Women Fearing Gender-Based Violence, India, August 2025' (UK Home Office, 18 December 2025).

ISSN: 2582-6433

Third, the federal government must pass a comprehensive federal data privacy bill that puts structural limits on the amalgamation and commercial sale of personal information the piping that supports the practice of doxing, identity theft, and targeted harassment campaigns on women. A good template could be found in the DPDP Act 2023 of India, which, however, needs its independence provisions to be reinforced.

Fourth, the two jurisdictions ought to invest in AI-related regulatory abilities such as AI-generated content detection tools, mandate of AI-generated media watermarking, and the mandatory prior study of gender implications by AI developers before the implementation of generative tools. The EU AI Act (2024) that mandates creators of deepfakes to label the products of AI helps to establish an international reference point.

Fifth, there should be substantial increase in law enforcement training, victim support infrastructure, and awareness programmes in the two countries. The most severe gap in India lies between the legal frameworks and the available enforcement capability: an advanced statutory framework can be of limited use when police stations have no technical capability to take and investigate complaints of cybercrime, and when the social norms are wary of allowing women to do so.[26]

CONCLUSION

The age of digital has become a paradox of women empowerment: those very platforms and technologies that have helped the access to education, economic opportunities, and a political presence have simultaneously provided new avenues in which gender-based violence can be perpetrated in a new scale and with new techniques, that is more exact, more scalable, and potentially more psychologically destructive. This paradox has become even more acute due to AI, which allows being harassed on an industrial level with the lowest technical threshold and the largest number of victims. The comparative analysis which has been made on India and the United States shows that both nations have acknowledged the challenge and made effective legislative measures in 2022-2025 as yet, yet both are still below the quickly changing pace of technology and experience of women in the digital space.

The recently adopted legislation wave in India the BNS 2023, the DPDP Act 2023 and DPDP Rules 2025, as well as the IT Rules 2021 are an important normative step; however, lacking

[26]SabrangIndia, 'India's Gender-Based Violence Crisis 2025: Facts Must Drive Change' (SabrangIndia, 9 September 2025) <https://sabrangindia.in/indias-gender-based-violence-crisis-2025-facts-must-drive-change/> accessed 1 March 2026.

ISSN: 2582-6433

both specific NCII legislation and dedicated enforcement infrastructure and the lack of survivor support means are limiting factors. The VAWA 2022, the take it down act, and the pending deferential act of the United States is a more victim-centered interpretation of technology-enabled gender-based violence, but weaken due to the lack of comprehensive data privacy protection and ongoing application of platform immunity dogmas.

The fundamental revelation which has come out of this comparative analysis is that, online gender-based violence is no longer a regulatory issue, it is a structural result of digital ecosystems that have been developed without considering the safety of women to be a priority. Environmentally friendly solutions do not include only new criminal and civil laws, but a complete change in the design of platforms, AI models, data management, and policing culture to the idea that ensuring women safe and equal participation in the digital public space is a constitutional and human right imperative. [27]

[27]National Association of Attorneys General, 'Congress's Attempt to Criminalize Nonconsensual Intimate Imagery: The Benefits and Potential Shortcomings of the TAKE IT DOWN Act" (NAAG, August 2025) <https://www.naag.org/attorney-general-journal/congresss-attempt-to-criminalize-nonconsensual-intimate-imagery-the-benefits-and-potential-shortcomings-of-the-take-it-down-act/>.