TECHNOLOGY-FACILITATED SEXUAL VIOLENCE AGAINST WOMEN IN INDIA: ARTIFICIAL INTELLIGENCE, DIGITAL HARM, AND THE LIMITS OF LAW

Ms. Chandni Dhawan[1] & Dr. Anmol Kaur Nayar[2]

ABSTRACT

"I didn't know why I was going to cry, but I knew that if anybody spoke to me or looked at me too closely, the tears would fly out of my eyes and the sobs would fly out of the throat, and I would cry for a week," a few words once shared by Sylvia Plath in her work The Bell Jar.[3]

The experiences this path captures are not unknown: navigating areas where openness is often a shared presence rather than a sense of cordiality and aid. In modern times, such vulnerability has extended beyond physical spaces, encroaching into virtual environments where exposure is amplified and harm is magnified.

This transition from material to digital space is not only about location, but also structure. Digital space can be conceptualised as an architecture of visibility sustained by platform architecture, algorithms, ordering, and data persistence. Where space visibility in a traditional sense is fleeting and circumstantial, digital space visibility is persistent, searchable, and reproducible. This makes the state of vulnerability qualitatively different from its presence in a traditional space; rather than a circumstantial experience, it is now a persistent one.[4]

The observation that digital technologies should not be seen as innocent intermediaries but as sites within which social relationships are negotiated, enhanced, and ultimately reproduced was also echoed in recent publications

[1] BA LLB, Amity Law School, NOIDA, Uttar Pradesh
[2] Associate Professor, Amity Law School, NOIDA, Uttar Pradesh
[3] Bridie Dillon, "Heart wrenching Quotes from Sylvia Plath That Keep Me Alive and Sane", *Medium*, Feb. 21, 2022, available at https://medium.com/youness-ness/heartwrenching-quotes-from-sylvia-plath-that-keep-my-alive-and-sane-fc4b4668e20 (last visited on Apr. 24, 2026).
[4] Alexandros Schismenos, *Artificial Intelligence & Barbarism: A Critique of Digital Reason* (Athens School, Athens, 2025).

by Agyare (2025)[5] and Prado (2025)[6]. platforms' algorithms often amplify gendered abuse through engagement-driven visibility.

Gendered Nature of Digital Harm

In the same way, Narayani (2024)[7] and Sankhwar et al. (2023)[8] render digital violence in relation to larger socio-economic structures, thus positioning women's experiences of digital violence as constantly intertwined with offline inequalities. This articulation of the digital space also goes some way toward establishing that it is not a discrete space but rather a reflection of the world outside, in terms of power dynamics, gendered spaces, and inequitable access.

Reports published by the UN and several Indian empirical studies highlight that, although the Indian Constitution asserts women's equality, women remain vulnerable in the digital space as digital inclusion increases.[9][10][11][12][13][14]

Between 16-58% women in India have been victims of various forms of digital abuse[15]

[5] Patrick Agyare, "Gendered Digital Harms and Youth Ideological Trajectories: SocioEconomic Challenges of Digital Platforms" 9(3) *SocioEconomic Challenges* 77 (2025), available at https://doi.org/10.61093/sec.9(3).77-96.2025 (last visited on Apr. 24, 2026).

[6] Elena López-de-Arana Prado, "Reconceptualising the Digital Gender Divide: Accommodating New Forms of Virtual Gender-Based Violence" 15(11) *Behavioral Sciences* 1568 (2025), available at https://doi.org/10.3390/bs15111568 (last visited on Apr. 24, 2026).

[7] Aditi Narayani, "Women's Safety in Digital Space" 70 *Indian Journal of Public Administration* 546 (2024), available at https://doi.org/10.1177/00195561241271513 (last visited on Apr. 24, 2026) (examining the link between digital privacy and women's empowerment in India, highlighting legal gaps, cyber harms, and the need for gender-sensitive policy and design interventions).

[8] Shweta Sankhwar, Rupali Ahuja, Tanya Choubey, Priyanshi Jain, Tanusha Jain & Muskan Verma, "Cybercrime in India: An Analysis of Crime Against Women in Ever Expanding Digital Space" 7(1) *Security and Privacy* e340 (2024), available at https://doi.org/10.1002/spy2.340 (last visited on Apr. 24, 2026) (analysing rising cybercrimes against women in India through statistical methods, identifying vulnerability patterns and geographic trends, and proposing preventive frameworks to address digital harms).

[9] Syed Faraz Akhtar & Moumita Datta Bhowmik, "Digital Violence: The Rise of Online Gender-Based Violence Against Women in the Age of Social Media" 7(2) *International Journal for Multidisciplinary Research* (2025), available at https://doi.org/10.36948/ijfmr.2025.v07i02.41785 (last visited on Apr. 24, 2026) (examining the rise of online gender-based violence in India, highlighting legal fragmentation, sociocultural drivers, and proposing reforms including stronger legislation, digital literacy, and platform accountability).

[10] UNESCO, "Providing Women with Digital Skills is Not Just About Inclusion—It is About Unlocking Their Full Potential and Ensuring Equal Opportunities in the Modern World" (2021), available at https://www.unesco.org (last visited on Apr. 24, 2026).

[11] UNESCO, "Challenges of Digital Literacy in Rural and Marginalized Communities" (2022), available at https://www.unesco.org (last visited on Apr. 24, 2026).

[12] UN Women, "Women in Low-Income Countries are 20% Less Likely than Men to Use the Internet, Further Widening the Digital Divide" (2022), available at https://www.unwomen.org (last visited on Apr. 24, 2026).

[13] United Nations, "Ensuring Women's Digital Inclusion is Not Just a Matter of Rights but a Necessity for Economic and Social Development in the Digital Age" (2022), available at https://www.un.org (last visited on Apr. 24, 2026).

[14] Amandeep Kaur, Alka Kumari & Gautam Negi, "The Impact of Digital Literacy on Women's Empowerment" 7(2) *International Journal for Multidisciplinary Research* (2025).

[15] UN Women, "Digital Violence is Real Violence: One Activist's Fight for Safety and Human Rights", *UN*

(Sankhwar et al., 2023; Pawar, 2025)[16], ranging from cyberstalking to unauthorised distribution of intimate images and videos (revenge porn), image morphing, deep-fake pornography and targeted online harassment. The very wide range itself suggests many underreported cases, possibly due to existing stigma, lack of awareness, and fear of character defamation.

Choudhary (2022)[17] and Muthukumar (2024)[18] are also swift to highlight that this brand of cybercrime operates within a broader social and cultural milieu that both feeds into the harm and is, in turn, affected by it, including how the issue is handled.

The evidence that the psychological effects of such cyber-enabled actions range from states of sadness and worry to complete withdrawal from virtual communities indicates that these cybercrimes have physical effects beyond the physical and virtual spaces in which they are committed.

AI and the Transformation of Harm

At the same time, artificial intelligence has further transformed the nature of such harm. With the existence of several technologies, the creation of synthetic media that automates abuse and rapid dissemination has made it easy for harm to occur on a scale and speed that even the most well-thought-out laws and legal frameworks are unable to keep pace with. Moreover, these technologies have been deployed and labelled as tools for cybersecurity, content moderation, and investigation, leading to a complex dynamic in which one can witness artificial intelligence functioning both as a producer of harm and a protection mechanism.

The extension of AI into the digital space has also exacerbated these problems. This process of making synthetic media, especially deep fakes by AI empowered devices, further

Women, Nov. 18, 2025, available at https://www.unwomen.org/en/news-stories/feature-story/2025/11/digital-violence-is-real-violence-one-activists-fight-for-safety-and-human-rights (last visited on Apr. 24, 2026) (emphasising the real-world impact of online abuse and highlighting systemic gaps in addressing digital violence against women).

[16] Aarti S. Pawar, "Cyber Crime and Female Victims in India: A Growing Crisis in the Digital Age" 13(3) *Gurukul International Multidisciplinary Research Journal* (2025), available at https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0002 (last visited on Apr. 24, 2026).

[17] R. Choudhary, "Cyberspace and Women: Dimensions of Cybercrime Against Women in India" *Design Engineering* (2022), available at https://doi.org/10.17762/de.vol2022iss1.8685 (last visited on Apr. 24, 2026) (examining the scope and nature of cybercrimes against women in India, highlighting patterns of online abuse and structural gaps in legal responses).

[18] Deepika Muthukumar, "Cybercrime Against Women in India" 6(6) *International Journal for Multidisciplinary Research* (2024), available at https://www.ijfmr.com/papers/2024/6/31857.pdf (last visited on Apr. 24, 2026).

erodes the concept of reality versus fiction, and as Sharma (2024)[19] and Cheng (2024)[20] also observed, this tech has become increasingly used as a tool for the production of non-consensual media with the concept of consent, identity and autonomy in the digital sphere.

Meanwhile, AI is also being used more frequently as a regulatory tool through the development of filtering and detection devices. The studies by Manche et al. (2025)[21] and Nazakat & Malik (2025)[22] center on using AI to identify problematic content, enabling faster responses. Still, their dual function raises troubling questions of responsibility when autonomous processes cause or exacerbate damage.

So, a paradoxical situation has arisen in which the AI is both the instrument of infliction and the remedy for that infliction, meaning the legalistic notion of determining exactly where the responsibility lies cannot be resolved.

Two aspects of this situation have started serious debates about who is responsible for the actions. It is uncertain if the person who uses the technology, the service that hosts and shares the content or the computer instructions that allow the information to spread is at fault. Due to those two roles, the legal environment is divided, and current laws do not easily determine who is liable when automated systems or artificial intelligence cause damage. By looking at the cases, the fact that legal regulations are not clear or do not address those specific problems is now a primary subject of attention.

[19] Himani Ahlawat & Somlata Sharma, "Cyber Crimes Against Women in India" 5(6) *ShodhKosh: Journal of Visual and Performing Arts* (2024), available at https://doi.org/10.29121/shodhkosh.v5.i6.2024.2430 (last visited on Apr. 24, 2026) (analysing forms of cybercrime targeting women in India, their socio-legal impact, and highlighting gaps in existing legal frameworks and enforcement mechanisms).

[20] Xiangshu Cheng, "The Gendered Impact of Deepfake Technology: Analyzing Digital Violence Against Women in South Korea" *Lecture Notes in Education Psychology and Public Media* (2024), available at https://doi.org/10.54254/2753-7048/75/20241102 (last visited on Apr. 24, 2026) (examining the gendered harms of deepfake technology, particularly its role in facilitating digital violence against women and reinforcing structural inequalities).

[21] Rahul Manche, FNU Samaah, Tejaswini Bollikonda & Praveen Kumar Myakala, "Empowering Safe Online Spaces: AI in Gender Violence Detection and Prevention" 10(2) *Journal of Science and Technology* 39 (2025), available at https://doi.org/10.46243/jst.2025.v10.i02.pp39-50 (last visited on Apr. 24, 2026) (examining the role of AI in detecting and mitigating gender-based online violence, while highlighting challenges such as algorithmic bias, privacy concerns, and the need for ethical and regulatory frameworks)

[22] Tooba Nazakat & Faiza Eiman Malik, "Empowering Justice through AI: Addressing Technology-Facilitated Gender-Based Violence with Advanced Solutions" 7(1) *Journal of Law & Social Studies* 26 (2025), available at https://doi.org/10.52279/jlss.07.01.2642 (last visited on Apr. 24, 2026) (examining the role of AI in addressing technology-facilitated gender-based violence and proposing advanced legal and technological interventions to strengthen justice mechanisms).

Victim, Barriers and Access to Legal Remedies

Moreover, beyond the issues surrounding the law and technology, it is the victim's experiences themselves that serve as the catalyst for all of this. This raises the question of why women face significant barriers in reporting their abuses in sexual digital crimes, as they lack awareness of their redressal mechanisms available to them, the fear of stigma and concerns regarding their privacy and social repercussions are some of the most cited reasons. In addition to these reasons, there exist instances where harmful content can remain accessible for an unaccountable extended period, despite it being reported, contributing to ongoing harm and secondary victimisation for the women who fall prey to such acts. Notably, the most prone to grooming, catfishing, and coercion, often without institutional support, are the young individuals of our nation.

Cybercrimes in India are regulated by the Information Technology Act, 2000[23] (in addition to some provisions of the Indian Penal Code, 1860[24] (Now amended by the Bharatiya Nyaya Sanhita, 2023[25]) and by the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.[26]

I do not seek to diminish or undermine the technological advances, nor do I wish to cast an enchantment that AI is an 'evil entity'. Instead, this has attempted to critically evaluate whether the manmade legal regimes in India integrating the use of AI are strong enough to successfully advance cybersecurity as well as protect the female victims of digital sexual crimes, in addition to examining whether they satisfactorily manage the complexities brought about by the newer technologies.

With the increasing integration of digital-based technology into everyday life, many crimes underwent a transformation in their nature in the context of gender, based violence. Primarily, India's expansion of internet access and social media use led to increased participation and new forms of vulnerability for women in digital spaces.

The transformation placed pressure on existing legal frameworks, particularly those under the Information Technology Act, 2000 and the Indian Penal Code, which were not

[23] Information Technology Act, No. 21 of 2000 (India)
[24] Indian Penal Code, No. 45 of 1860 (India).
[25] Bharatiya Nyaya Sanhita, No. 45 of 2023 (India)
[26] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.

designed to regulate such technologically mediated harms.

The growing magnitude of digital participation cannot be reduced to numbers; instead, we are witnessing a transformation not only in participation but also in its configuration. In these circumstances, access to and utilisation of the internet by women are thus subject to, and will be severely limited by, state monitoring and regulation. Prado (2025) further takes this as an extension of the digital gender divide by arguing that 'inclusion in the digital realm does not mean inclusiveness and can, through this paradox, be an extension of digital inequality.

The increasing prevalence of technology-based harms, and the slippery slope of digital abuse, is a concern. Amongst these are cyberstalking, nonconsensual distribution of sexually exploitative images, targeted harassment and other newer forms of threats such as deep fake porn, which are forms of online violence and have robbed women of their right to dignity online, caused them emotional and reputational harm and disconnected them from the net.

Choudhary (2022) and Muthukumar (2024) argue that it would be unfair to classify these acts as cybercrimes, as they are rooted in sociocultural frameworks in which protocols of victim-blaming and patriarchy influence the submission and acknowledgement of such conduct by and within institutions.

Though there is an awareness of such harms existing, existing scholars have largely maintained their writing of texts and concepts on bringing forth the prevalence of such forms of abuse and the social and cultural factors, like stigmas and underreporting. While the scholars' contributions are integral to understanding the concept and addressing it, the studies do not sufficiently examine how victims would navigate legal and technological systems after the harms they faced, nor evaluate how effectively these systems provided meaningful redress. This creates a critical gap between documenting harm and evaluating institutional effectiveness in addressing it.

Chandel and Sethi (2025)[27] from a systemic perspective highlights paradoxically wider issues encountered with Cyber Laws in India. Sheikh and Rogers (2023)[28] show that victims

[27] Jyoti Chandel & Aruna Sethi, "Judicial Interpretation and Enforcement Challenges in Addressing Cyber Crimes Against Women in India" 5(4) *International Journal of Advanced Research in Science, Communication and Technology* 476 (2025), available at https://doi.org/10.48175/ijarsct-29961 (last visited on Apr. 24, 2026) (examining judicial responses and enforcement challenges in cybercrime cases involving women, highlighting gaps in interpretation and implementation of existing legal frameworks).

[28] Md. Mamunur Rashid Sheikh & Michaela M. Rogers, "Technology-Facilitated Sexual Violence and Abuse in

were affected psychologically with feelings of anxiety, depression, and feelings of rejection from both the digital and physical spaces. The lack of familiarity with the technologies and processes involved worsens the grim future that the victims face.

From a systemic perspective, Chandel and Sethi (2025) point out that, paradoxically, wider problems are faced with cyber laws in India. Even when legal texts are in place, enforcement and interpretation are flawed due to misapplication, insufficient awareness of technological advances, and delays in legal processes. The dearth of their understanding of the technologies and processes involved enhances the victim's plight.

The incorporation of artificial intelligence into digital environments has only added to the environment's intricacy. While AI-powered platforms facilitate the creation of malicious and synthetic content and enable harmful practices, they are also used for content moderation and detection. This raises concerns about accountability, responsibility, and the sufficiency of current regulatory structures.

In this way, as a piece of writing, the is in the space where law, technology and lived experience meet. It endeavours to understand whether the existing law, platform and AI-enabled responses in India are sufficiently equipped to enable adequate protection, provide redress and deliver long-term support to victims of technological facilitation of sexual violence against women.

The expanding adoption of digital technologies has significantly shaped cybercrime and its impact on women and society in the digital age, transforming the forms, scale and persistence of violence against women and increasingly shifting such harm into online spaces. The scale, persistence, and mechanisms of such violence have evolved considerably. There has been an important rise in cybercrime against women, accompanied by a growing body of literature attempting to understand this phenomenon. However, the approach and response to this new form of violence against women differ significantly across existing literature.

However, Saraswati (2024)[29] indicates that, in fact, the real magnitude of such crimes

Low and Middle-Income Countries: A Scoping Review" 25(2) *Trauma, Violence, & Abuse* 1614 (2024), available at https://doi.org/10.1177/15248380231191189 (last visited on Apr. 24, 2026) (examining the prevalence and patterns of technology-facilitated sexual violence in low- and middle-income countries, highlighting structural vulnerabilities and gaps in legal and policy responses).

[29] Vibha Saraswati, "Navigating Cybercrime: The Impact on Women in India and the Need for Digital Safety" 13(6) *International Journal of Science and Research* (2024), available at

against women may be far larger, as women feel ashamed to report them due to the social stigma involved. Hence, it may be conceded that cybercrimes against women are on the rise, and many cases may go unreported, but the exact scale of this problem is not known.

Also, Ahlawat and Sharma (2024) make an important observation: the growing instances of cybercrime against women are a reason for the lower participation of women in online public spaces, a matter of concern for inclusivity and equity. However, their analysis focuses on the consequences rather than the structural causes of such an undesirable outcome. A significant portion of the existing work relies heavily on the harm caused by cybercrime against women, but often lacks in analysing how the law operates on the ground.

The existing literature denotes that cyber violence against women overall is a consequence of the lacunae in the law, outmoded societal attitudes towards gender and the role of digital technologies and the online ecosystem, yet it fails to adequately examine the interaction between these variables and how the scope and operation of the Information Technology Act, 2000 and the Intermediary Guidelines and Digital Media Ethics Code) In 2021, the rules were further weakened in their enforcement.

Moving beyond the issue of physical violence in a digital environment, a contemporary commentary, such as that presented in the Noosphere Substack[30], suggests that technological systems actively shape social behaviour and, in doing so, 'set the tone' for unwanted and abusive behaviour in the online ecosystem, making it 'normal' to indulge in such behaviour. This resonates with the literature on the role and agency of the online world in propagating social harms.

While the literature on cybercrimes against women, no doubt, provides an in-depth understanding and an extensive catalogue of the scale and intensity of the crimes, there is a lacuna in comprehending the long-term impact of such crimes, and an understanding of how effective the legal regimes are in bringing them to an end. This chapter endeavours to address these issues.

https://doi.org/10.21275/sr24623193426 (last visited on Apr. 24, 2026) (examining the rise of cybercrimes against women in India, highlighting psychological harm, underreporting due to stigma, and the need for digital literacy and stronger legal awareness mechanisms).

[30] Katie Jagielnicka, *The Noösphere* (Substack), available at https://thenoosphere.substack.com (last visited on Apr. 24, 2026)

The literature agrees about women as uniquely affected within the digital sphere; however, scholars utilize disparate methods in the theorizing of such vulnerabilities. Balabantaray et al (2023)[31] focuses on the implications of wider internet usage while Dar and Nagrath (2022)[32] focus on systemic inequalities. While both are important lenses, without referring to Ahlawat and Sharma (2024), who frame cybercrimes as limiting women's access and participation in the digital realm, each view is potentially guilty of individualising vulnerability.

From a legal perspective, cybercrimes fall under the IT Act, as well as sections of the IPC. These offenses are addressed by the various provisions of Section 66E and 67[33] of the IT Act, 2000 as well as penal code provisions for harassment, stalking etc. However, most of these provisions are not designed to address technology-induced harms, such as AI- or synthetic content-based harms.

On the other hand, in the literature, very few works have addressed the extent to which these statutory provisions are implemented in relation to cybercrimes. In this sense, some major restrictions, such as significant delays in proceedings, jurisdictional issues, and the production of evidence, are ignored.

In this context, judicial interpretation has also responded to the threat of cybercrime against women. Judges have become more willing to recognise the harmful nature of online offences such as the unauthorised distribution of images and cyber-stalking, yet court decisions have been generally reactive and individualised and have not developed an overall doctrinal body addressing technologically based harm.

Patterns emerging from reported cases further demonstrate why such a narrow legal framework is inadequate. In many cases, abuse happens in interpersonal and intimate settings, in which digital space acts merely as a new platform for control and abuse. Online stalking and persistent harassment that occurs with the threat of disseminating sexually explicit material to

[31] Subhra Rajat Balabantaray, Mausumi Mishra & Upananda Pani, "A Sociological Study of Cybercrimes Against Women in India: Deciphering the Causes and Evaluating the Impact on the Victims" 19(1) *International Journal of Asia Pacific Studies* 23 (2023), available at https://doi.org/10.21315/ijaps2023.19.1.2 (last visited on Apr. 24, 2026) (analysing socio-economic and structural causes of cybercrime against women in India, examining victim impact, and highlighting systemic and reporting-related challenges).
[32] S. A. Dar & D. Nagrath, "Are Women a Soft Target for Cyber Crime in India" 3(1) *Journal of Information Technology and Computing* 23 (2022), available at https://doi.org/10.48185/jitc.v3i1.503 (last visited on Apr. 24, 2026) (examining the vulnerability of women to cybercrime in India and highlighting systemic, social, and technological factors contributing to targeted online abuse).
[33] Information Technology Act, 2000, §§ 66E, 67.

private persons, along with other threats of physical harm, continue even with the help of digital communications that serve to bolster the claim that such crimes are not anonymised or detached.

Cases concerning younger victims also readily depict features of post, relationship abuse, the sharing of images of people in sexual situations, together with the digitally false portrayal of the victim's age and identity. The facts of these cases imply that current legislation does not recognise the ongoing and evolving nature of abuse in the cyber world, and there is likely a need for a broader approach that does not require dividing cybercrime into individual criminal offences. In fact, the behaviour seems to consist of a series of harmful actions rather than categories of crime like those described in the literature.

Technology-facilitated sexual violence (TFSV)

In the body of the literature, 'technology-facilitated sexual violence' (TFSV) was the new, umbrella term developed as an understanding of the violation online.

Henry and Powell (2018)[34] have defined TFSV in terms of behaviors, including harassment, coercion, and image-based abuse. Patel and Roesch (2020)[35] and Henry, Flynn, and Powell (2020)[36] have reiterated and expanded these parameters with respect to mental health and socio-cultural consequences.

However, despite collectively contributing to defining the scope and consequences of TFSV, each scholarship has done so from different angles (e.g., some from categorisation and others from impact), and there has been a general lack of interaction with legal translation within a specific context, such as India.

[34] Nicola Henry & Anastasia Powell, "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research" 19(2) *Trauma, Violence, & Abuse* 195 (2018), available at https://doi.org/10.1177/1524838016650189 (last visited on Apr. 24, 2026) (providing a foundational analysis of technology-facilitated sexual violence, identifying patterns of online abuse and highlighting gaps in legal and empirical responses).

[35] Unnati Patel & Ronald Roesch, "The Prevalence of Technology-Facilitated Sexual Violence: A Meta-Analysis and Systematic Review" 23(2) *Trauma, Violence, & Abuse* 428 (2020), available at https://doi.org/10.1177/1524838020958057 (last visited on Apr. 24, 2026) (providing empirical evidence on the prevalence of technology-facilitated sexual violence, highlighting its widespread nature and reinforcing the need for stronger legal and policy responses).

[36] Nicola Henry, Asher Flynn & Anastasia Powell, "Technology-Facilitated Domestic and Sexual Violence: A Review" 26(14) *Violence Against Women* 1828 (2020), available at https://doi.org/10.1177/1077801219875821 (last visited on Apr. 24, 2026) (reviewing the intersection of technology with domestic and sexual violence, highlighting patterns of digital abuse and the need for integrated legal and policy responses).

Although the notion of technology-assisted sexual assault builds a robust narrative within the context of digital injury, its use in the Indian legal framework seems minimal.

The translation of such concept frameworks into rights has, at the level of legal literature, failed to provide an interface. Such conceptual frames have not been successfully translated into legal rights in legal literature, creating an interface between them.

Digital Platforms and Intermediary Liability

In academia, the importance of digital platforms to cybercrime has become an area of increased discussion.

Dehingia et al. (2023)[37] discussed the increase of online misogyny, and Adrija Dey (2023)[38] framed digital harassment as an extension of real-world violence and explained how platforms were more than simple conduits and an amplifier. Pain (2020)[39] and Nanditha (2021)[40] have further strengthened the argument by providing examples of how even activist spaces have exclusion.

With regard to the law, that is, the intermediary liability is provided by the IT Act and specifically the 2021 Rules. Orders that are legal problematic can be seen as the main reason for internet crime regulating difficulty, especially with the courts having trouble fulfilling the orders and injunctions to take down the harmful content. For example, one of the cases against Google ordered the removal of AI-generated and altered material, the URL to the material, as

[37] N. Dehingia, J. McAuley, L. McDougal, E. Reed, J. Silverman, L. Urada & A. Raj, "Violence Against Women on Twitter in India: Testing a Taxonomy for Online Misogyny and Measuring Its Prevalence During COVID-19" 18 *PLOS ONE* (2023), available at https://doi.org/10.1371/journal.pone.0292121 (last visited on Apr. 24, 2026) (empirically analysing online misogyny on Twitter in India, developing a taxonomy of abuse and measuring its prevalence, particularly during the COVID-19 period).

[38] Adrija Dey, "It's a Joke, Not a Dick. So Don't Take It Too Hard: Online Sexual Harassment in Indian Universities" 24(8) *Feminist Media Studies* 1830 (2024), available at https://doi.org/10.1080/14680777.2023.2266150 (last visited on Apr. 24, 2026) (examining normalization of online sexual harassment in Indian university spaces and highlighting cultural and institutional factors that enable gendered digital abuse).

[39] Paromita Pain, "It Took Me Quite a Long Time to Develop a Voice: Examining Feminist Digital Activism in the Indian #MeToo Movement" 23(11) *New Media & Society* 3139 (2020), available at https://doi.org/10.1177/1461444820944846 (last visited on Apr. 24, 2026) (examining feminist digital activism in India, highlighting how online platforms enable women's voices while also exposing them to backlash and structural inequalities).

[40] Nanditha N., "Exclusion in #MeToo India: Rethinking Inclusivity and Intersectionality in Indian Digital Feminist Movements" 22(8) *Feminist Media Studies* 1673 (2021), available at https://doi.org/10.1080/14680777.2021.1913432 (last visited on Apr. 24, 2026) (critiquing the limitations of inclusivity within India's #MeToo movement, highlighting intersectional gaps and structural exclusions in digital feminist discourse).

well as the platforms to take down the URLs, but the fact that the original material could be re-uploaded demonstrates that the takedown mechanisms are not efficient in controlling the digital harm replicability.

The IT Rules, 2021 require intermediaries to comply with due diligence principles, such as removing illegal content when they are alerted. Yet, this arrangement clearly is far from being achieved as some of the content was not removed and was easily uploaded again.

The essential defect in the intermediary liability schemes is seen by depending solely on the notice-and-takedown mechanisms that are reactive; these schemes are unable to deal with the persistent and reproducible character of harm on the internet without the need to directly tackle the platform design that is creating the loophole.

Emergent Harms: Artificial Intelligence and Deepfakes

The nature of cybercrime is shifting rapidly due to emerging technology, primarily artificial intelligence. As indicated by Thumboo and Mukherjee (2024)[41], digital technologies facilitate insidious forms of abuse; indeed, analyses, such as that conducted for Make It Real: AI-Facilitated Gendered Harm (2025)[42], confirm that more than three-quarters of all AI-generated content is specifically used against women, predominately through the creation of non-consensual imagery and deepfakes.

Illustrative events underline the severity of these risks; it was widely reported that an image of multiple women was manipulated using AI to create defamatory, obscenely suggestive images.

Judicial responses have confirmed both the threat and inadequacy of current legal systems. Courts recognise AI-generated sexual content as a serious issue and have ordered it to be taken down; victims are often granted anonymous status, and ordering website owners to disable illegal content is becoming more commonplace. However, there have been repeated

[41] S. Thumboo & S. Mukherjee, "Digital Romance Fraud Targeting Unmarried Women" 2 *Discover Global Society* (2024), available at https://doi.org/10.1007/s44282-024-00132-x (last visited on Apr. 24, 2026) (examining the gendered dynamics of online romance fraud, highlighting how unmarried women are specifically targeted through emotional manipulation and digital deception).

[42] Siddharth Pillai, Tarunima Prabhakar & Kaustubha Kalidindi, *Make It Real: Mapping AI-Facilitated Gendered Harm* (Rati Foundation & Tattle Civic Tech, 2025), available at https://tattle.co.in/make-it-real-report.pdf (last visited on Apr. 24, 2026) (analysing AI-facilitated gendered harms using survivor-based evidence, highlighting emerging abuse patterns and systemic gaps in legal and platform responses).

takedowns for images such as that in Mrs. X V. Union of India[43] without halting circulation of harmful content.

Procedural frameworks are also beginning to acknowledge and compensate for the shortcomings in the law, for example with the standard operating procedures (2022) on deepfake cases identifying growing instances and insufficient solutions.[44]

The growth in size and complexity of cybercrime driven by AI, is outpacing the legal remedies the law can respond with in terms of attribution as well as prevention.

Research Gaps in Existing Literature

Further, in the field of cybercrime against women, legal, technological and socio-cultural dimensions are often discussed in isolation with the absence of a comprehensive and integrated approach. The nexus among these three dimensions has been addressed only sporadically. More specifically, very few research papers have examined how institutional mechanisms respond to AI-caused harm, particularly regarding their implementation and effectiveness. Research in this area has largely focused on how cybercrimes occur, their types, and their social and cultural effects. There have been limited attempts to examine whether and how existing legislation and regulations operate in practice.

Moreover, while the legal, technological, and socio-cultural dimensions have been explored in the literature, they are rarely analysed in an integrated manner, and their interrelationships are often addressed only in a fragmented way.

Reimagining Law in the Age of Artificial Intelligence

There is a consensus in the literature that the occurrence and severity of cybercrimes against women is high, but there is still a significant deficiency regarding their legal and systemic nature. This disconnects between harm and response forms the foundation of the

[43] *Mrs. X v. Union of India*, 2023 SCC OnLine Del 2361 (Delhi High Court, decided on Apr. 26, 2023) (issuing directions to intermediaries, MeitY and police authorities for prompt removal and redressal in cases of non-consensual dissemination of intimate images).

[44] Aayushman Gaikwad & Smruti Mishra, "India's New Rules for AI-Generated Content and Deepfakes", *LiveLaw* (Feb. 21, 2026), available at https://www.livelaw.in/articles/ai-generated-content-deepfakes-524064 (last visited on Apr. 24, 2026) (discussing regulatory changes introducing stricter obligations on intermediaries, including mandatory labelling of AI-generated content, traceability requirements, and significantly reduced takedown timelines for unlawful deepfake content).

present study. This gap becomes particularly significant in the context of artificial intelligence, where existing legal frameworks remain largely reactive and insufficient to address technologically mediated harm.

As demonstrated, the problem of AI-enabled cybercrime facing women is not one of legal inadequacy but of structural deficiency and systemic failure. The problem is not simply the absence of law, but the absence of the right sort of law.

This underestimate is driven by one undeniable but profound truth: the law still functions in spaces that were never meant to, and never could be, meant to recognise harm done in the digital realm, let alone damage done through AI. Extensions of laws like the Information Technology Act and criminal law done by the judiciary have been piecemeal, intuitive, and unlikely to be forward-looking: Instead of acknowledging that the very definition of harm has changed, the law tries to go back and infuse it with new exceptions.

This leaves individuals, particularly women, unable to find a meaningful sense of place within the system. There is a stark distinction between the types of crime, where rights, remedies, and procedures are fairly understood, and AI-enabled abuse, which exists in an unsettled legal landscape. In situations where individuals endure image morphing, deepfake production, or digital circulation without consent, they cannot hope to find a mechanism to obtain redress. The law lacks a pragmatic "box" to identify the flow of harm, label it, and respond to it. The question thereby becomes not whether the harm happened, but whether the system is in fact able to recognise that it happened.

This question, indeed, is further complicated by the intimate and precise nature of the problem caused by this harm. The harm is not only a legal one; it is also a social, psychological, and personal shadow. That social stigmatization which arises from such personal experiences becomes the major barrier for women in speaking out against the problem. The emotional impact and threats of secondary victimisation generally outweigh the potential benefits of legal redress, such that secondary victimisation can often block the legal route altogether.

Even in instances where individuals pursue the legal route, the lack of confidence in data security, confidentiality, and the sensitivity of the various institutions involved impairs trust in the enforcement mechanism. Currently, the debate is not simply whether the claimant will get justice, but whether, in attempting to do so, the claimant will simply be another victim.

The drawback to this situation is reinforced by the legal system's reactive nature. Protection is only granted after harm and only to those who have the consciousness, the resources and the social standing that make their ability to access legal remedies. A deeply stratified system emerges, such that those most vulnerable to harm are also those least able to avail themselves of protection. The victims often do not know they have been harmed until the circulation has already spread. By that time, the damage to their identity, status, and stature is, for all intents and purposes, permanent.

If the situation described above is not the responsibility of a single mechanism or actor, then it would seem to be the responsibility of Facebook itself, along with the State, legal institutions, and, perhaps most broadly, society. The State has failed to influence technological change through proactive legal adaptation. Although legal institutions attempt to adapt through interpretation, they are constrained by inadequate internal structures. Despite having technically advanced tools to recognise and curtail harm, platforms are also driven by a business model that creates engaging flows in which harm circulates quickly. Society, for its part, normalises and perpetuates harm (in relation to women in particular).

What we see emerging from this analysis is not a call for reform, but for reimagination. The law needs to begin by recognising AI-enabled abuse as a specific form of harm which cannot be efficiently classified under rulings on obscenity, defamation or privacy. Its lack of clarity results in slippery-slope debates, weak enforcement, and absent deterrence. It is necessary for the law to create an accessible, specific structure to categorise nonconsensual online identity adjustment.

Secondly, the approach to regulation must become more proactive than reactive. The model currently used, victims wait to see the damage, identify, and contact authorities, is structurally defective. Protection cannot be on victims' being careful or aware, or knowing how to report abuse. It must be built into the technology itself. In other words, legislation should encourage systems that detect and block harmful content early and intervene quickly when issues arise online. Moreover, one more thing is that giving online platforms a free pass should not be the case. They are not mere pipes that deliver things from A to B. Platforms decide what millions see, tell certain stories, and shape online conversations.

Therefore, they should be accountable for what appears. Just replying to complaints is too little, too late. Firms need to consider how their platforms exacerbate situations (mainly

through recommendation engines and sorting), what their systems do, and introduce clear rules and measures to prevent the spread of abuse. Regarding the law and our response to AI damage, there should be a dedicated team or agency that works closely with people who know the tech. With the right experts and judges, complaints can be processed more quickly and fairly. Whoever is in charge should put people first, making sure that victims' information stays confidential, that help is readily available, and that those affected by online abuse are supported.

On a larger scale, the law must also grow to accommodate this increased sophistication of dignity, as well as technological progress and understanding. There are new dimensions to the ways an individual can suffer harm, for example, not just through physical conduct but through the circulation and alteration of their digital identity, which can impact their psychological sense of worth. The protection of this form of personal dignity will require a move away from existing legal categories, and a recognition of this right to digital dignity and integrity as a fundamental Human Right:

In the final analysis, it is not about the law's ability to cope with AI-enabled harm, but about its corresponding capacity to reconfigure itself towards this goal. No piece of amendments will do. What is needed is a leap in 'mindset and infrastructure', from a nature and purpose that is reactive, to one that is proactive; from a paradigm that is fault, or wrongdoing, oriented, to one that is systemic, and environment-centric; and from a tentative, prescriptive, conditional dispensation, to one that is certain, and quantitative.

Thus, this concludes that the future of legal regulation in this field will be in redefining the relationship between law and technology rather than merely extending it within existing boundaries. To achieve meaningful protection, it is only through this redefinition that law can move beyond the acknowledgement of harm.