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 or copied in any form by any means without prior written permission of Managing Editor of IJLRA. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of IJLRA.

Though every effort has been made to ensure that the information in Volume II Issue 7 is accurate and appropriately cited/referenced, neither the Editorial Board nor IJLRA shall be held liable or responsible in any manner what sever for any consequences for any action taken by anyone on the basis of information in the Journal.

ISSN: 2582-6433

EDITORIALTEAM

EDITORS

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

Dr. Namita Jain

Head & Associate Professor
School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC-NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India. India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi. (2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

ISSN: 2582-6433

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr.Sagunthala R & D Institute of Science and Technology, Avadi. Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship. He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi. Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi. He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN- 2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

ISSN: 2582-6433

PROTECTING WOMEN IN INDIA'S CYBER SPACE

AUTHORED BY - AAYUSH VERMA
Research Scholar, Department of Law, School of Legal Studies, Babasaheb Bhimrao Ambedkar University, Lucknow

CO-AUTHOR - PROF. (DR.) SUDARSHAN VERMA
Head, Department of Law, School of Legal Studies, Babasaheb Bhimrao Ambedkar University

CO-AUTHOR 2 - BHAVYA MITTAL
LL.M., Department of Law, School of Legal Studies, Babasaheb Bhimrao Ambedkar University, Lucknow

ABSTRACT

The digitalisation of Indian society has opened new possibilities for communication, business, and social interaction, but it has also shaped unique and sophisticated dangers, particularly for women who faces harassment, doxxing, the non-consensual circulation of intimate images, sexualised trolling, and even frauds like digital arrest scams. These experiences are not just technical crimes; they are deeply tied to patriarchal norms, social stigma, and structural inequalities that leave women with lasting harm like psychological distress, social exclusion, and financial loss which often silence their voices online. While India's cyber laws, such as the Information Technology Act, 2000, and newer provisions in the Bharatiya Nyaya Sanhita, 2023, represent themselves as gender-neutral but in reality, they fall short of recognising the specific ways women are targeted and harmed. Even Judiciary, in the landmark K.S. Puttaswamy v. Union of India case, have acknowledged rights to privacy, dignity, and equality, but there are still glaring gaps in both legal recognition and enforcement when it comes to online gender-based violence. This research paper addresses the requirement for the shift of focus from treating the offences as an isolated offences to understanding them as part of a larger system of "digital patriarchy." This requires placing women's experiences at the heart of legal responses, ensuring trauma-informed procedures, confidential and accessible reporting mechanisms, and more robust institutional support systems. It also means grounding constitutional values like dignity, privacy, and equality in cyber, while ensuring accountability

ISSN: 2582-6433

from online platforms and building mechanisms for international cooperation against transnational crimes like digital arrest scams. Beyond the law, there is an urgent need for cultural change through digital literacy and awareness programs, especially for women in vulnerable communities, to dismantle stigma and empower women to participate fully and safely in India's digital future.

Keywords- Cyberspace, Feminist Legal Theory, Cyber Crimes, Digital Arrest, Harassment.

INTRODUCTION

The rapid digitalisation of Indian society has significantly reshaped modes of communication, commerce, and social interaction. However, parallel to these transformative benefits, cyberspace has simultaneously emerged as a critical site for gendered violence and exploitation. Women face excessive threats that range from online harassment, doxxing, non-consensual circulation of intimate images, and sexualised trolling to newer and more treacherous forms of cyber fraud such as digital arrest scams. These offences exploit structural inequalities, patriarchal anxieties, and social stigma surrounding women's sexuality, thereby heightening their vulnerability within the digital ecosystem[1]. The rapid expansion of internet penetration has further allowed perpetrators to conceal themselves behind digital anonymity, thereby evading traditional mechanisms of accountability. According to the National Crime Records Bureau, cybercrimes against women consistently increased between 2018 and 2022, with cyberstalking and publication of obscene material comprising a key share. Particularly alarming is the rise in extortion through fabricated videos or impersonation, in which women have been the primary targets[2]. The outcomes of these crimes are deep psychological trauma, social shunning, and financial exploitation resulting in the silencing of women's participation in digital spaces[3].

Against this setting, feminist legal theory becomes a crucial lens for examining cybercrimes against women. While traditional legal frameworks appear gender-neutral in wording, they are often gender-biased in effect, failing to account for patriarchal structures embedded in cyberspace that imitate offline inequalities online. A feminist perspective insists not only on protection from harm but also on the empowerment of women to exercise independence and

[1] National Crime Records Bureau, Crime in India 2023 (Ministry of Home Affairs, Government of India, 2023).
[2] National Crime Records Bureau, Crime in India 2022 (Ministry of Home Affairs, Government of India, 2022).
[3] National Commission for Women, Annual Report on Cyber Crimes Against Women (NCW, New Delhi, 2021).

ISSN: 2582-6433

dignity in digital environments[4]. In India, where deep-rooted social norms often stigmatise women who report such crimes, feminist jurisprudence insists for laws that confront not just the offences but also the systemic barriers that discourage women from seeking justice. The objectives of this paper are first, to trace the evolution of cybercrimes against women in India, from typical forms of harassment to sophisticated scams like digital arrests; second, to critically evaluate the adequacy of the Information Technology Act, 2000 and related provisions of the Bharatiya Nyaya Sanhita, 2023; and third, to explore feminist perspectives on digital safety, establishing responsibility on both the State and private actors to create a gender-sensitive cyberspace. The research seeks to answer three central questions: How do cybercrimes against women uniquely manifest in Indian cyberspace? Are Indian legal frameworks effective in addressing these gendered harms? What would a feminist framework for cyber security require, and how might it strengthen constitutional guarantees of dignity, equality, and privacy[5] ? Consequently, this paper positions cybercrime not merely as a technological or legal issue but as a constitutional and feminist concern, emphasising that protecting women in cyberspace must move beyond the prevention of offences to safeguarding their digital dignity as an essential component of constitutional morality.

THEORETICAL FRAMEWORK: FEMINIST LEGAL PERSPECTIVE

The legal structure governing cyber offences in India is mainly framed as gender-neutral. However, neutrality that ignores structural inequalities tends to obscure, rather than dismantle, patriarchal domination. Feminist legal theory provides an indispensable lens for examining crimes against women in cyberspace, exposing the limitations of existing frameworks and reimagining a gender-just cyber dominion. At its core, feminist jurisprudence argues that law is not an impartial authority but a social construct shaped by historical power irregularities. In India, legal interpretation and enforcement have long reflected a male-centric worldview, frequently marginalising women existed realities. When this approach extends to cyberspace, digital crimes targeting women are treated as anomalies rather than as manifestations of rooted hierarchies. Online harassment, often sexualised in nature, aims to police women's public participation, echoing offline patriarchal restrictions[6].

Intersectionality deepens this analysis by revealing how women from marginalised

[4] Catharine A. MacKinnon, Toward a Feminist Theory of the State 98 (Harvard University Press, Cambridge, 1989).
[5] K.S. Puttaswamy v. Union of India, AIR 2017 SC 4161.
[6] Supra note 4 at 2.

ISSN: 2582-6433

communities Dalits, minorities, and LGBTQ+ individuals face distinctive risks of cyber violence[7]. Patriarchy adapts to technological platforms, producing digital gender-based violence that is amplified by anonymity, permanence of digital records, and rapid dissemination. Online spaces thus replicate structural inequalities, silencing women through trolling, body-shaming, propagation of intimate images, and threats of sexual assault. Such violence nullifies women's political participation and curtails their citizenship in digital democracies[8]. The phenomenon of digital arrest scams is illustrative: perpetrators impersonating state authorities exploit women's fear of social stigma, reputational harm, and institutional victim-blame. While these scams are supposedly gender-neutral, their operation is profoundly gendered, leveraging patriarchal notions of shame and honour to coerce compliance[9].

Indian cyber laws primarily the Information Technology Act, 2000 and relevant provisions of the Bharatiya Nyaya Sanhita, 2023 remain fragmentary and reactive. They criminalise discrete offences such as obscenity, impersonation, and voyeurism but fail to address the structural asymmetries that render women extremely vulnerable. The absence of explicit recognition of online gender-based violence as a distinct legal category reflects the male-centric design of these statutes[10]. Enforcement is crammed with patriarchal bias. Police frequently downplay or dismiss complaints, discouraging women from filing FIRs. This reproduces the silencing effect historically seen in the treatment of sexual offences, where survivors were subjected to moral scrutiny while perpetrators escaped accountability[11]. In cyberspace, the effect is deepened by weak institutional capacity for gender-sensitive cyber policing, which further entrenches mistrust in legal remedies.

Constitutional Principles and Feminist Reimagination

A feminist legal perspective resonates with constitutional guarantees of equality, dignity, and privacy. Article 14[12] mandates not only objective but substantive equality, compelling the State to account for gender-specific harms in digital environments. Article 21's guarantee of dignity

[7] Kimberlé Crenshaw, 'Mapping the Margins: Intersectionality, Identity Politics, and Violence Against Women of Color' 43(6) Stanford Law Review 1241 (1991).
[8] Anja Kovacs, Internet Democracy Project Report: Cyber Crimes Against Women in India (2018).
[9] National Commission for Women, Annual Report (NCW, New Delhi, 2021).
[10] Usha Ramanathan, 'Cyber Crimes and the Information Technology Act' 39(5) Economic and Political Weekly 4059 (2004).
[11] Flavia Agnes, 'Protecting Women Against Violence? A Review of a Decade of Legislation' 27(17) Economic and Political Weekly WS19 (1992).
[12] The Constitution of India, art. 14.

ISSN: 2582-6433

and privacy as affirmed in *Justice K.S. Puttaswamy v. Union of India*[13] that extends to protecting women's "digital dignity" against doxxing, harassment, and the unauthorised circulation of private material. Similarly, while the Supreme Court in *Shreya Singhal v. Union of India*[14] addressed the chilling effect of vague cyber laws on free speech, a feminist reading emphasises that unfettered digital spaces themselves silence women by enabling harassment and intimidation. A balanced constitutional vision is therefore necessary that safeguards cyber freedoms while simultaneously mandating proactive state responsibility to guarantee women's equal and safe participation in digital spheres.[15]

Applying feminist jurisprudence to cybercrime demands three normative shifts. First, law must move beyond individualised offences to a structural recognition of digital patriarchy as systemic. Second, remedies must prioritise victim-centred justice, including accessible reporting mechanisms, anonymity protections, and trauma-informed support, rather than relying solely on punitive sanctions. Third, constitutional morality must inform cyber governance, embedding dignity, equality, and privacy as non-negotiable anchors of regulation. The feminist perspective reframes cybercrimes against women not as isolated misuses of technology but as constitutional failures to secure gender justice in a digitised society.[16]

EVOLUTION OF CYBER CRIMES AGAINST WOMEN IN INDIA

The course of cybercrimes against women in India reflects the shifting contours of technology, social behaviour, and patriarchal control. In the late 1990s and early 2000s, reported offences were largely confined to online obscenity, tampering with electronic communications, and email abuse. However, as internet penetration deepened, the band of gendered offences widened to include cyber harassment, stalking, voyeurism, revenge porn, financial frauds, and most recently, digital arrest scams. These offences reveal the dual reality of India's digital revolution as access to technology has expanded opportunities, it has at the same time created grave risks for women's safety and dignity. Cyber harassment has remained the most reported form of online violence, ranging from abusive emails and defamatory messages to constant trolling on social media. According to the NCRB, nearly 70% of cyber complaints filed by women pertained to harassment, stalking, or bullying, with young women between 18–30 years

[13] K.S. Puttaswamy v. Union of India, AIR 2017 SC 4161.
[14] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[15] Ibid.
[16] Supra note 4 at 2.

ISSN: 2582-6433

disproportionately affected[17].

A particularly concerning development has been the non-consensual circulation of intimate images (NCII), often referred to as revenge porn or deepfakes. With smartphones and affordable internet, cases of morphed images, abusive memes, and pornographic content have risen significantly, with the NCRB recording a 25% increase in offences under Sections 67 and 67A of the IT Act between 2017 and 2021[18]. The landmark case of *State of West Bengal v. Animesh Boxi*[19], where the accused was convicted for creating a fake profile with morphed images, underscored the devastating impact of NCII on women's dignity and mental health. Despite judicial recognition of harm, India still lacks comprehensive legislation addressing NCII, leaving many victims unprotected. Similarly, financial scams have strangely targeted women through fake matrimonial websites, phishing, and employment frauds. The NCW noted that scammers frequently exploit gender norms by trapping women with promises of marriage or employment, then resorting to extortion or blackmail using objectionable material[20]. Such exploitation thrives on the patriarchal stigma surrounding women's sexuality, rendering female victims more vulnerable compared to their male counterparts.

More recently, digital arrest scams have emerged as a sophisticated and crafty threat. In these scams, fraudsters impersonate law enforcement officers, pressuring women into prolonged video calls where they are "digitally confined" and extorted under the guise of bail or investigation. These scams, which gained visibility in metropolitan cities like Delhi, Mumbai, and Bengaluru during 2022–2023, disproportionately affect women, who are more likely to comply due to fears of reputational harm, police harassment, or social stigma. Despite their increasing incidence, digital arrest scams fall into a jurisdictional gap, as neither the IT Act nor the BNS provides a clear framework to prosecute such offences. Offenders often operate transnationally, using encrypted platforms and cryptocurrency, which makes tracking and prosecution exceedingly difficult in the absence of robust international cooperation mechanisms.

The NCRB reported 52,974 cybercrime cases nationwide, with nearly one-third involving

[17] National Crime Records Bureau, Crime in India 2020 (Ministry of Home Affairs, Government of India, 2020).
[18] National Crime Records Bureau, Crime in India 2021 (Ministry of Home Affairs, Government of India, 2021).
[19] State of West Bengal v. Animesh Boxi, 2018 SCC OnLine Cal 237.
[20] Supra note 3 at 2.

ISSN: 2582-6433

harassment and financial fraud against women[21]. Similarly, the NCW cyber helpline recorded 17,000 complaints in 2021 alone, reflecting a sharp rise due in part to pandemic-induced digital reliance[22]. Judicial interpretations have developed incrementally, relying on provisions such as Section 78 BNS (cyberstalking) and Section 79 BNS (insulting the modesty of a woman), with constitutional jurisprudence most notably *K.S. Puttaswamy v. Union of India*[23] by fortifying the recognition of privacy violations as constitutional harm. Still, enforcement remains erratic, hindered by victim-blaming attitudes, underreporting, and the lack of specialised cyber units. Mapping the evolution of cybercrimes against women reveals distinct phases: early email abuse and obscenity (2000s), the expansion of harassment and trolling (2010s), escalation through revenge porn and phishing (2015–2020), and the current phase of transnational scams such as digital arrests (post-2020)[24]. Each stage reflects how patriarchal anxieties adapt to technological platforms, underscoring the need for re-evaluation of cyber regulation that addresses not only the offences but also the structures enabling women's vulnerability in cyberspace.

LEGAL FRAMEWORK IN INDIA: AN ANALYSIS

India's legal framework addressing cybercrimes against women lies at the intersection of the Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, and the procedural safeguards of the Bharatiya Nagarik Suraksha Sanhita (BNSS). While these statutes reflect progressive amendments and judicial interventions, challenges of enforcement, gender-sensitivity, and jurisdiction persist, making a feminist legal analysis indispensable. The IT Act, India's first consolidated legislation on computer-related offences, includes critical provisions such as Section 66E (privacy violations), Sections 67–67B (obscenity and sexually explicit material), Section 72 (breach of confidentiality), and Sections 66C–66D (identity theft and impersonation). These provisions directly or indirectly address harms like voyeurism, revenge porn, and frauds such as digital arrest scams. Still, the Act has faced criticism for its ambiguity, overbroad powers, and inadequate effectiveness in providing remedies for gendered harms.

Complementing the IT Act, the criminal laws especially following the Nirbhaya case and Justice Verma Committee recommendations has expanded to explicitly cover cyber-enabled

[21] Supra note 2 at 2.
[22] National Commission for Women, Cyber Complaint Data (NCW, New Delhi, 2022).
[23] National Commission for Women, Cyber Complaint Data (NCW, New Delhi, 2022).
[24] Singh, Richa, 'Digital Dignity and Feminist Appr Richa Singh, 'Digital Dignity and Feminist Approaches to Cyber Harassment' 63(1) Journal of the Indian Law Institute 25 (2021).

ISSN: 2582-6433

offences. Sections 74, Section 76 and Section 78 addressing sexual harassment, stalking, voyeurism, and also criminalising cyberstalking via electronic communication. Section 356 cover defamation, Section 79 penalises insults to women's modesty, and Sections 294–296 address obscenity in online contexts. These sections acknowledge the gendered nature of cyber offences, while Section 351(4) addresses anonymous threats an increasingly common form of online intimidation. Despite these legal advances, gaps in enforcement, lack of awareness among investigating agencies, and procedural delays have hindered their real-world efficacy.

The procedural framework under the BNSS is crucial in determining jurisdiction, investigation, and prosecution of cybercrimes. Sections 197 and 199 deal with jurisdiction in offences spanning multiple locations, yet cross-border cybercrimes continue to expose deficiencies in India's extradition protocols and mutual legal assistance treaties mechanisms (MLAT). Specialised cybercrime cells have been established across states, though gender-sensitive policing remains unreliable. The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, place obligations on intermediaries to regulate harmful content, but enforcement remains uneven, with platforms often inconsistent in curtailing misogynistic or abusive material[25]. This lack of accountability has multiplied women's vulnerability in digital spaces.

Judicial interpretation has further shaped the contours of India's cyber law regime. In *Shreya Singhal v. Union of India*, the Supreme Court struck down Section 66A of the IT Act as unconstitutional while underscoring the importance of safeguarding women from digital abuse[26]. In *K.S. Puttaswamy v. Union of India*, the Court recognised privacy as a fundamental right, providing constitutional grounding for redress against digital privacy violations[27]. Similarly, in *State of West Bengal v. Animesh Boxi*, the Calcutta High Court convicted an offender for circulating morphed images of a woman, recognising the severe impact on dignity[28]. The systemic challenges like underreporting due to social stigma, victim blaming, lack of gender-sensitive policing, jurisdictional hurdles in transnational offences, and legislative gaps regarding emerging threats such as deepfake pornography or digital arrest scams continues to undermine the law's ability to effectively protect women online[29].

[25] Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021.
[26] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[27] K.S. Puttaswamy v. Union of India, AIR 2017 SC 4161.
[28] State of West Bengal v. Animesh Boxi, 2018 SCC OnLine Cal 237.
[29] Supra note 2 at 2.

ISSN: 2582-6433

CASE STUDY: DIGITAL ARREST SCAMS AND WOMEN VICTIMS

Digital arrest scams signify a noxious and rapidly evolving form of cybercrime that mainly targets women by exploiting deep-rooted socio-cultural stigmas, fear of law enforcement, and technological vulnerabilities[30]. These scams involve fraudsters impersonating police or government officials through calls, emails, or video conferencing platforms, coercing victims into believing they are implicated in fabricated criminal cases that demand immediate monetary payments for bail or investigation aid. Victims are often digitally confined during the extortion process are kept on continuous calls, threatened with arrest, and shamed with the spectre of social disgrace. Such manoeuvres cause psychological trauma alongside financial loss, highlighting how technological manipulation intersects with gendered social vulnerabilities[31].

Defined as a subset of online fraud and extortion, digital arrest scams are characterised by the misuse of state authority symbols to intimidate and isolate victims[32]. Leveraging VoIP systems, anonymised communication apps, and cryptocurrency transactions, perpetrators achieve a high degree of invisibility, enabling cross-border operations that evade traditional enforcement tools[33]. Women are disproportionately targeted due to patriarchal norms that stigmatise women in any legal or moral controversy, regardless of innocence. Fear of dishonour, out casting, and inadequate institutional support make them uniquely vulnerable to intimidation. In many cases, women are silenced by the weaponisation of "shame," compelled to comply with scam demands swiftly and discreetly. This reveals the intersection of patriarchal power structures with new-age digital extortion techniques[34].

Reported incidents have surged in metropolitan centres such as Delhi, Mumbai, Bengaluru, and Hyderabad, prompting public advisories by cybercrime cells and state police departments[35]. However, case numbers remain underreported due to society and distrust in institutional redressal. Legal recourse is further complicated by statutory ambiguities and though the provisions such as BNS Section 319 (cheating by impersonation), Section 351 (criminal intimidation), and Section 66D of the IT Act (impersonation) may apply, prosecuting cross-border perpetrators is cumbersome and delayed[36]. Jurisdictional and technical hurdles worsen

[30] Supra note 9 at 4.
[31] Supra note 24 at 7.
[32] National Commission for Women, Annual Report (NCW, New Delhi, 2022).
[33] Ibid.
[34] Supra note 24 at 7.
[35] Delhi Police Cyber Cell, Public Advisory on Digital Arrest Scams (2023) (unpublished report).
[36] Ministry of Home Affairs, Cyber Crime Enforcement Challenges Report (Government of India, 2023).

ISSN: 2582-6433

enforcement gaps. The transnational nature of these scams, combined with encryption technologies and cryptocurrency-based payments, makes existing investigative frameworks ineffective. India's mutual legal assistance treaties and extradition protocols remain inadequate, while domestic cybercrime cells often lack the technical capacity to trace sophisticated operations[37].

From a feminist jurisprudential perspective, the state's response reflects broader systemic inadequacies in protecting women in cyberspace. Awareness campaigns, though increasing in number, fail to address the patriarchal fear structures that scammers exploit, and victim support infrastructure remains insufficient[38]. Women frequently encounter insensitive policing, victim-blaming, and social ostracism, deterring them from reporting such offences[39]. Effective reform requires specialised cybercrime tribunals with confidential, victim-sensitive procedures; robust international treaties for cross-border prosecution; capacity-building for cyber police units with gender-sensitive and trauma-informed training; public–private partnerships with digital platforms for real-time scam alerts; and nationwide digital literacy campaigns to empower women against manipulation[40]. Ultimately, digital arrest scams epitomise how cybercrime intersects with gendered vulnerabilities, exposing gaps in India's regulatory landscape[41].

COMPARATIVE PERSPECTIVE: ADDRESSING ONLINE GENDER-BASED VIOLENCE

The ever-increasing challenge of online gender-based violence (OGBV) has led several jurisdictions, including the United Kingdom, European Union, and United States, to design legislative and policy responses designed to the realities of digital harms faced by women. These frameworks vary in scope and strategy but share a common emphasis on platform accountability, victim protection, and gender-sensitive enforcement. Studying these comparative approaches will provide India with valuable lessons for refining its cybercrime laws and institutional architecture to respond more effectively to technology-facilitated gendered violence.

The United Kingdom has emerged as a leader through the enactment of the Online Safety Bill

[37] Ministry of External Affairs, Mutual Legal Assistance Treaties Annual Report (Government of India, 2023).
[38] Supra note 24 at 7.
[39] Apar Gupta, 'Law Enforcement and Women Victims of Cybercrime in India' 9 NUJS Law Review 120 (2021).
[40] Internet Freedom Foundation, Policy Recommendations for Cyber Safety (2023).
[41] Supra note 24 at 7.

ISSN: 2582-6433

(OSB), 2023, which introduces a statutory duty of care for internet service providers to safeguard users against harmful content, explicitly including sexual harassment and gender-based abuse[42]. The Bill mandates companies to proactively moderate harmful material, ensure rapid takedowns of illegal content, and publish transparency reports. Gender-based harassment is recognised as a priority category, mandating targeted interventions by platforms and embedding a framework that balances victim protection with corporate responsibility. The OSB empowers 'Ofcom' as an independent regulator with authority to impose significant penalties and issue compliance directions, while also prioritising user empowerment through reporting tools and digital literacy programs. This reflects a holistic, victim-centred regulatory design.

The European Union, by contrast, employs a multi-pronged approach anchored in the Budapest Convention on Cybercrime[43] for cross-border cooperation and the Digital Services Act (DSA), 2022[44], which regulates online intermediaries. The DSA imposes obligations of transparency, systemic risk assessment, and harm mitigation on digital platforms along with gender-based violence recognised as a specific area of concern. What separates the EU model is its integration of human rights and gender equality principles into technological regulation, requiring Member States not only to adopt gender-sensitive criminal laws but also to establish institutional support services for victims of online violence. This dual focus on prevention and redress demonstrates a rights-based and socially responsive governance framework.

In the United States, the strategy is shaped by a combination of federal statutes and state-level initiatives, including provisions under the Violence Against Women Act[45] and laws criminalising cyberstalking, revenge porn, and online harassment. Agencies such as the Federal Communications Commission and Federal Trade Commission further regulate illusory practices and scams in the digital sphere, complementing criminal law responses. Significantly, the US approach recognises intersectionality by addressing how vulnerabilities linked to race, ethnicity, and sexual orientation exacerbate women's exposure to online abuse. The model also balances civil remedies and privacy protections with strong enforcement measures, while fostering public-private collaboration with social media companies and implementing digital literacy campaigns to build resilience against OGBV.

[42] UK Government, Online Safety Bill (2023).
[43] Council of Europe, Budapest Convention on Cybercrime (2001).
[44] European Parliament, Digital Services Act (2022).
[45] Violence Against Women Act, 1994 (USA), as amended.

ISSN: 2582-6433

TOWARDS A FEMINIST LEGAL FRAMEWORK FOR CYBER SAFETY IN INDIA

The digital age has modified public and private boundaries, deepening the need for a legal framework responsive to the gendered nuances of cybercrime. India's existing laws, though progressively amended, remain largely gender-neutral and reactive, falling short of addressing the specific vulnerabilities and lived realities of women in cyberspace[46]. A feminist legal framework demands a consolidative approach grounded in constitutional ethos, embedding principles of substantive equality, autonomy, privacy, and dignity. Recognising cyber violence against women as a human rights violation. This approach situates cyber safety within the guarantees of equality, non-discrimination, and liberty under Articles 14, 15, and 21 of the Indian Constitution, thereby establishing "digital dignity" as central to women's rights[47].

Such a framework must operationalise constitutional morality by accounting for how intersecting identities of caste, class, and sexuality shape women's experiences of cyber harm[48]. Legal reforms should therefore revise the Information Technology Act and Bhartiya Nyaya Sahinta to include gender-explicit provisions, definitions for emerging offences such as deepfakes, digital arrest scams, and online coercion, and the removal of victim-blaming tendencies that discourage women from seeking justice. A victim-centric legal regime requires the institution of specialised cyber violence tribunals, cyber forensic units with gender-sensitive expertise along with trauma-informed reporting procedures designed to prevent secondary victimisation. Swift removal of offending content and mandatory intermediary compliance would further enhance women's access to effective redress[49].

At the preventive level, feminising cyber law also requires a broader cultural shift. Comprehensive digital literacy programmes must be scaled up, particularly in rural and marginalised communities, equipping women and girls with tools for online safety[50]. Public awareness campaigns dismantling patriarchal myths around women's digital behaviour are essential to counter stigma and encourage reporting. Alongside this, digital platforms must be held accountable through enforceable obligations on transparency, content moderation, and

[46] Supra note 24 at 7.
[47] The Constitution of India, arts. 14, 15, 21.
[48] Supra note 7 at 3.
[49] Ministry of Home Affairs, Cyber Crime Investigation Guidelines (Government of India, 2023).
[50] Ministry of Electronics & IT, Digital Literacy Campaign (Government of India, 2023).

ISSN: 2582-6433

equitable grievance redressal mechanisms to curb harassment and hate speech[51]. These measures should be supplemented by enhanced international cooperation, as the cross-border nature of cybercrimes such as digital arrest scams and deepfakes necessitates India's active engagement in treaties like the Budapest Convention, bilateral cyber agreements, and collaborations with global technology companies to facilitate data-sharing, extradition, and joint investigations.

The effective operationalisation of a feminist cyber legal framework depends on clearly defined roles for all stakeholders. Police forces must undergo regular gender-sensitivity and technical training to build trust in enforcement processes, while the judiciary should develop interpretative guidelines grounded in constitutional morality to protect women's digital rights robustly. Digital platforms, telecom operators, and intermediaries must also bear legal responsibility for ensuring safer online ecosystems. Constructing such a framework is not merely about criminalisation, but about embedding empowerment, prevention, and systemic reform into law. By centring constitutional guarantees of equality and dignity, strengthening institutional capacities, expanding digital literacy, and fostering international cooperation, India can transform cyberspace into a domain where women's rights are proactively protected and their digital dignity is upheld[52].

CONCLUSION AND RECOMMENDATIONS

The course of cybercrimes against women in India has evolved from early instances of online harassment and obscene content dissemination to complex, transnational threats such as digital arrest scams, deepfakes, and financial frauds. These harms violate privacy, dignity, and financial security while reinforcing entrenched patriarchal controls across both digital and physical spheres. Although India's legal framework anchored in the Information Technology Act, 2000 and Bhartiya Nyaya Sahinta, 2023 has made incremental progress but it still remains largely gender-neutral and reactive, leaving significant gaps in addressing the gendered nature of digital harms. Feminist jurisprudence demonstrates that formal equality is insufficient without substantive equality that accounts for women's vulnerabilities and intersectional identities. Constitutional morality, as articulated in *K.S. Puttaswamy v. Union of India*[53] and related jurisprudence, demands that women's digital dignity be recognised as intrinsic to

[51] Internet Freedom Foundation, Platform Accountability Report (2023).
[52] K.S. Puttaswamy v. Union of India, AIR 2017 SC 4161.
[53] K.S. Puttaswamy v. Union of India, AIR 2017 SC 4161.

ISSN: 2582-6433

constitutional rights to privacy, equality, and liberty. Empirical trends reveal that offences such as cyberstalking, revenge porn, and fraudulent schemes are facilitated by patriarchal stigma and systemic underreporting[54]. While judicial interventions have strengthened rights to privacy and free expression, persistent issues of victim-blaming, inadequate police sensitisation, and the inability to effectively trace cross-border offenders[55] underscore the urgent need for legal and institutional reform.

Addressing these challenges requires a feminist-informed cyber law architecture that is proactive, intersectional, and constitutionally anchored. Comprehensive gender-specific legislation should explicitly recognise and criminalise gender-based digital offences, including non-consensual image circulation, deepfake misuse, and coercive fraud targeting women[56] (Singh 2021). Institutional reforms are equally necessary, including specialised cybercrime tribunals, dedicated forensic units, and trauma-sensitive reporting mechanisms designed to reduce secondary victimisation[57]. Preventive measures must prioritise nationwide digital literacy initiatives tailored to women and marginalised groups, complemented by public awareness campaigns to dismantle patriarchal narratives around women's online presence[58]. Regulatory frameworks should mandate digital intermediaries to maintain transparency, enforce responsible content moderation, and establish accessible grievance redressal mechanisms, drawing from models such as the UK's Online Safety Bill[59]. At the international level, India must strengthen treaty-based cooperation and actively engage with conventions such as the Budapest Convention while enhancing bilateral mechanisms with global enforcement agencies and technology platforms[60]. Ultimately, safeguarding women's digital futures requires transcending gender-neutral, reactive enforcement and embracing a transformative feminist legal framework that ensures safe, inclusive, and empowering digital spaces where women can exercise their constitutional rights with dignity and equality.

India could benefit from codifying a statutory duty of care that obliges digital intermediaries to actively detect and remove abusive gendered content, drawing from the OSB and DSA

[54] Supra note 1 at 2.
[55] Ministry of External Affairs, Mutual Legal Assistance Treaties Report (Government of India, 2023).
[56] Supra note 24 at 7.
[57] Supra note 39 at 9.
[58] Supra note 50 at 12.
[59] Supra note 40 at 10.
[60] Interpol, Global Cybercrime Trends Report (2023).

ISSN: 2582-6433

models. Establishing an independent regulatory authority with enforcement powers would strengthen accountability and instil greater confidence among victims. Embedding a human rights-based and gender equality-oriented framework within cyber to ensure that laws respond to the lived realities of women. India must strengthen cross-border cooperation mechanisms, drawing from the EU's Budapest Convention experience, to effectively prosecute transnational crimes such as digital arrest scams. Adopting a victim-centred approach through dedicated helplines, specialised courts, protection schemes, and inclusive digital literacy initiatives for rural and marginalised women to address systemic barriers and empower survivors to seek justice.