
A STATUTE STRANDED IN TIME: IRWA, THE IT ACT, AND THE REGULATION OF ONLINE GENDER-BASED HARM, EVIDENCE FROM MAHARASHTRA

Raghav Golhani & S.K. Deshmukh, Maharashtra National Law University, Nagpur

ABSTRACT

This paper examines the interface between the Indecent Representation of Women (Prohibition) Act, 1986 and the Information Technology Act, 2000 in addressing cyber-enabled gender-based violence against women in Maharashtra. It situates IRWA in its original print-media context and demonstrates how the rapid expansion of social media, image morphing, deepfakes, cyberstalking, and online sexual harassment has exposed the doctrinal and technological limits of a pre-digital statute. Using NCRB data from 2019 to 2023, parliamentary records and data, NCRP complaint data, and a comparative analysis of statutory definitions and punishment structures, the study documents rising cybercrime figures and demonstrates that complaints involving obscene or sexually explicit online content are now overwhelmingly registered under IT Act provisions, especially sections 67 and 67A, and BNS provisions, with IRWA playing only a marginal, supplementary role. The paper argues that while IRWA remains normatively important for its gender-specific focus on women's dignity, it is operationally obsolete for cyberspace unless substantially amended and harmonized with the IT Act. The study critically engages with existing scholarship, including the paper by Gurjalwar and Dixit published in the *Indian Journal of Law and Legal Research*, Volume VII Issue I, to identify gaps in the prior literature that this paper addresses through state-specific empirical analysis. The study concludes by proposing legal and institutional reforms, including digital amendments to IRWA, convergence mechanisms between IRWA and the IT Act, a specific deepfake offence, and enforcement improvements for Maharashtra.

Keywords: IRWA, Information Technology Act, Cybercrime Against Women, Maharashtra, Digital Gender-Based Violence, Legal Obsolescence, BNS 2023.

I. INTRODUCTION

The digital revolution has fundamentally transformed the landscape of communication, commerce, and social interaction in India. With 86.3 per cent of Indian households now possessing internet access, as documented by the Government's Comprehensive Modular Survey 2025,¹ cyberspace has become the primary arena not only for economic activity and democratic discourse but also for a new and pervasive form of gender-based violence. The proliferation of smartphones, affordable data plans, and social media platforms has created unprecedented opportunities for connection, but it has simultaneously generated new vectors for the harassment, objectification, and exploitation of women in digital environments.

The Indecent Representation of Women (Prohibition) Act, 1986 (hereinafter "IRWA") was enacted in an era when print media, motion pictures, and conventional advertising were the dominant forms of mass communication.² The statute's definitional core, section 2(c), focuses on the "figure, form, or body" of a woman as depicted in traditional media, and its operative prohibitions under sections 3 and 4 target advertisements and publications containing indecent representation.³ IRWA was a pioneering statute in 1986: it normatively anchored women's dignity in statutory law for the first time in India, recognising that the commodification of the female body in visual media constituted a distinct legal harm worthy of criminal sanction.

However, the statute predates the internet, social media platforms, deepfake technology, cloud storage, end-to-end encrypted messaging, and user-generated content. Cyberspace has produced entirely new forms of gender-based harm, image morphing, non-consensual intimate image sharing, cyberstalking, sextortion, deepfake pornography, and coordinated online harassment, that IRWA's 1986 architecture was never designed to address. The gap between the statute's textual reach and the technological reality of digital abuse has widened with every passing year, rendering IRWA increasingly marginal to the contemporary enforcement framework for cyber-enabled gender violence.

In Maharashtra, India's most urbanized and digitally connected state, cybercrime against women has grown sharply. NCRB data shows Maharashtra registered 8,103 cybercrime cases in 2023, accounting for approximately 9.4 per cent of the national total of 86,420 cases.⁴ The

¹ Ministry of Electronics and Information Technology, Comprehensive Modular Survey 2025 de(India).

² Indecent Representation of Women (Prohibition) Act, 1986, No. 60, Acts of Parliament, 1986, § 2(c) (India).

³ *Id.* §§ 3-4.

⁴ National Crime Records Bureau, CRIME IN INDIA 2023 (2024) (India).

state's combination of high internet penetration, dense urban populations, and a relatively active law enforcement apparatus makes it a particularly revealing site for empirical analysis of the statutory framework's effectiveness.

The IRWA Amendment Bill, 2012, which sought to extend the statute to digital media by incorporating the concept of "electronic form" and expanding its reach to internet-mediated content, was introduced in Rajya Sabha in December 2012.⁵ However, the Bill was withdrawn on 26 July 2021 without being passed, leaving the Act unchanged and its pre-digital architecture intact. This withdrawal represents a critical missed legislative opportunity and constitutes the structural explanation for IRWA's current technological obsolescence.

This paper critically evaluates IRWA's effectiveness in addressing cyber harassment in Maharashtra through four analytical lenses: (a) doctrinal analysis of the statutory provisions of IRWA, the IT Act, and the Bharatiya Nyaya Sanhita, 2023 (BNS); (b) empirical data from NCRB, NCRP, and parliamentary sources documenting the trajectory of cybercrime complaints and IRWA registrations; (c) a comparative analysis of the punishment structures under the three statutes; and (d) a critical engagement with prior scholarship, particularly the paper by Gurjalwar and Dixit published in this journal, to identify the gap that this paper fills.

The paper is guided by three research questions. First, to what extent is IRWA effective in addressing cybercrime against women? Second, what trends emerge from empirical data on cybercrime complaints by women in Maharashtra? Third, how do the IT Act and IRWA interact in addressing online gender-based violence? The paper's research hypothesis is that IRWA is inadequate to deal with the emerging phenomenon of cybercrime because it is a pre-technological statute, that there is a significant enforcement and awareness gap affecting case handling in Maharashtra even with supplementary IT Act and BNS provisions, and that major legislative reform is required.

II. LITERATURE REVIEW

A. Scholarship on IRWA and Its Pre-Digital Architecture

The statutory framework of IRWA and its pre-digital design have attracted sustained scholarly

⁵ The Indecent Representation of Women (Prohibition) Amendment Bill, 2012, Bill No. XLVIII-C of 2012 (India) (withdrawn July 26, 2021).

attention, though the body of peer-reviewed literature directly addressing the statute's application to cyber-enabled harms remains surprisingly thin. The foundational peer-reviewed article directly on point is Debarati Halder's *Examining the Scope of Indecent Representation of Women (Prevention) Act, 1986 in the Light of Cyber Victimisation of Women in India*, published in the National Law School Journal in 2013.⁶ Halder argues that while IRWA is gender-specific and normatively significant, uniquely targeting the dignity of women rather than obscenity in the abstract, its definitional architecture is anchored in print media and fails to address fake avatars, image morphing, and digital distribution channels. She contends that this gap must be bridged through "harmonious interpretation" with the IT Act, a doctrinal strategy that acknowledges IRWA's normative value while recognizing its textual limitations. Her analysis, written a decade before the present study, provides the doctrinal framework that this paper validates empirically with state-specific data from Maharashtra.

The Amendment Bill of 2012 sought to address the gap identified by Halder and other commentators by incorporating the concept of "electronic form" into IRWA's definitions and extending its operative prohibitions to internet-mediated content. However, as noted by legal commentators, the Bill's withdrawal in 2021 left the statute's pre-digital architecture entirely intact, confirming the structural obsolescence that Halder had anticipated.⁷

B. Cybercrime Against Women: Empirical and Criminological Literature

The empirical and criminological literature on cybercrime against women in India has developed substantially over the past decade. Halder and Jaishankar's *Cyber Crimes Against Women in India* (SAGE Publications, 2016) is the seminal Indian text.⁸ It catalogues the full spectrum of cyber-enabled harms, cyberstalking, trolling, image morphing, and revenge pornography, and finds that existing laws are riddled with loopholes that leave victims without adequate remedy. The work provides an essential empirical foundation but operates at the national level without disaggregating data by state or mapping complaint trajectories against specific statutory provisions.

⁶ Debarati Halder, *Examining the Scope of Indecent Representation of Women (Prevention) Act, 1986 in the Light of Cyber Victimisation of Women in India*, 11 Nat'l L. Sch. J. 188, 193–94 (2013).

⁷ *The Indecent Representation of Women (Prohibition) Act, 1986 in Time of Social Media*, iPleaders (July 31, 2024), <https://blog.ipleaders.in/the-indecent-representation-of-women-prohibition-act-1986-in-time-of-social-media/>.

⁸ Debarati Halder & K. Jaishankar, *Cyber Crimes Against Women in India* (SAGE Publications 2016).

Halder and Jaishankar's earlier comparative work on secondary victimization demonstrates that India's legal framework structurally produces underreporting through social stigma, police inaction, and the revictimization of complainants during the investigative process.⁹ K. Jaishankar's Space Transition Theory provides the theoretical basis for understanding why cyberspace produces distinct patterns of gender-based offending: identity flexibility, dissociative anonymity, and lack of deterrence in digital environments enable offenders to commit crimes they would not risk in physical space.¹⁰ This theoretical framework helps explain the empirical divergence documented in this paper between the declining use of IRWA and the rising volume of IT Act prosecutions, cyberspace offending operates under different psychological and structural conditions that a print-media statute cannot adequately address.

The NORC/ICRW report on technology-facilitated gender-based violence in India, published with USAID support in 2022, confirms that the IT Act is the primary legal recourse for victims of online abuse but does not explicitly address gender-based psychological violence, and that there is a significant enforcement gap between the statutory framework and the lived experience of victims.¹¹ The report's finding that law enforcement agencies frequently discourage women from filing complaints reinforces the underreporting dimension that contextualizes the empirical data analysed in Part IV of this paper.

C. IT Act Judicial Interpretation

The judicial interpretation of the IT Act's provisions on obscene and sexually explicit electronic content has been shaped by two landmark Supreme Court decisions. In *Shreya Singhal v. Union of India*, the Supreme Court struck down section 66A of the IT Act as unconstitutional for vagueness, while affirming the high threshold for restricting online speech under Article 19(2) of the Constitution.¹² The decision established that overbroad criminal provisions targeting online content violate the right to free speech and that any restriction must satisfy the tests of reasonableness and proportionality. While *Shreya Singhal* did not directly address IRWA, its analytical framework, requiring precise statutory definitions and a

⁹ Debarati Halder & K. Jaishankar, *Cyber Gender Harassment and Secondary Victimization: A Comparative Analysis of the United States, the UK, and India*, 6 Victims & Offenders 386, 391 (2011).

¹⁰ K. Jaishankar, *Space Transition Theory of Cyber Crimes*, in CRIMES OF THE INTERNET 283, 286 (Frank Schmallegger & Michael Pittaro eds., 2008).

¹¹ NORC at the Univ. of Chi. & Int'l Ctr. for Research on Women, Technology-Facilitated Gender Based Violence in India 4–5 (USAID 2022), <https://www.icrw.org/wp-content/uploads/2021/09/USAID-TFGBV-India.pdf>.

¹² *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).

demonstrated nexus to constitutionally permissible grounds of restriction, has significant implications for IRWA's vague definitional standards.

More recently, in *TVF Media Labs Pvt. Ltd. v. State of NCT of Delhi*, the Supreme Court, applying the community standard test from *Ranjit D. Udeshi v. State of Maharashtra*, quashed FIRs registered under sections 67 and 67A of the IT Act and sections 3 and 4 of IRWA, holding that the use of profane language does not satisfy the obscenity threshold and that section 67A requires a demonstrated sexually explicit act or conduct.¹³¹⁴ This is the most recent Supreme Court authority on the operative standards for IT Act and IRWA enforcement in digital contexts and establishes that both statutes require content to cross a threshold of explicit depiction rather than mere offensiveness.

D. Recent Regulatory and Parliamentary Developments

The institutional recognition of the inadequacy of existing frameworks has accelerated in recent years. The Parliamentary Standing Committee on the Empowerment of Women submitted its Fourth Report on “Cyber Crimes and Cyber Safety of Women” on 23 March 2026, finding a 239 per cent increase in cybercrimes against women between 2017 and 2022 and recommending a “comprehensive and gender-sensitive cybercrime law” that addresses the full spectrum of digital harms.¹⁵ The Committee's findings constitute the strongest institutional acknowledgment to date that the existing multi-statute framework, including IRWA, the IT Act, and the BNS, is insufficient to protect women in digital environments.

On the regulatory front, the IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, effective 20 February 2026, introduced a statutory definition of “synthetically generated information” and a two-hour takedown obligation for non-consensual intimate synthetic content on Significant Social Media Intermediaries.¹⁶ These Rules represent the most significant executive action on deepfake-related abuse to date, though they address intermediary obligations rather than individual criminal liability, a distinction that is further analysed in Part VII.

¹³ *TVF Media Labs Pvt. Ltd. v. State of NCT of Delhi*, 2024 SCC OnLine SC (India) (decided Mar. 19, 2024).

¹⁴ *Ranjit D. Udeshi v. State of Maharashtra*, AIR 1965 SC 881 (India).

¹⁵ Comm. on Empowerment of Women, *Fourth Report: Cyber Crimes and Cyber Safety of Women* (Mar. 23, 2026).

¹⁶ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026 (India) (effective Feb. 20, 2026).

E. Gap in the Literature and This Paper's Contribution

Existing scholarship, whether doctrinal (Halder 2013), criminological (Halder and Jaishankar 2016), or socio-legal (NORC/ICRW 2022), operates at a national or abstract level. There is a notable absence of state-specific empirical studies that disaggregate IRWA's operational trajectory against cybercrime complaint data. No published study has mapped IRWA's registration figures against IT Act cybercrime data in a single state to demonstrate the statute's empirical displacement.

Critically, the paper by Gurjalwar and Dixit published in the Indian Journal of Law and Legal Research, Volume VII Issue I, "Critical Analysis of the Indecent Representation of Women (Prohibition) Act, 1986 and Its Relation to Patriarchy", exemplifies this gap.¹⁷ The paper is purely doctrinal and makes no use of NCRB data, NCRP complaint figures, or parliamentary records. It misquotes IRWA's penalties, stating imprisonment of "up to three years and a fine of up to Rs. 2 lakhs" for first offences when section 6 in fact provides a maximum of two years' imprisonment and a fine of only two thousand rupees. It cites a fabricated "Section 354E IPC" that does not exist in the statute book, the 2013 Criminal Law Amendment introduced sections 354A through 354D only. It relies on a 1981 Ph.D. dissertation on male nudity in advertising as authority for contemporary claims about Indian films. These deficiencies are not merely technical errors but reflect the absence of rigorous empirical engagement that characterizes much of the existing IRWA scholarship.

This paper fills the gap: it is the first Maharashtra-specific empirical study to map IRWA's zero-complaint trajectory from 2018 to 2021 against rising IT Act prosecutions, thereby providing the empirical validation that Halder anticipated in doctrinal terms a decade ago. It also incorporates the most recent institutional developments, the Parliamentary Committee Report of March 2026 and the IT Amendment Rules 2026, that post-date all previously published scholarship on this topic.

III. THE IRWA: STATUTORY FRAMEWORK AND PRE-DIGITAL ARCHITECTURE

A. Original Legislative Intent

The Indecent Representation of Women (Prohibition) Act was enacted in 1986 when print

¹⁷ Ishita Anand Gurjalwar & Bhavya Dixit, *Critical Analysis of the Indecent Representation of Women (Prohibition) Act, 1986 and Its Relation to Patriarchy*, 7 Indian J.L. & Legal Rsch. 4581, 4586–87 (2025).

media, motion pictures, and conventional advertising were the dominant forms of mass communication in India.¹⁸ The Act's legislative goal was to address the objectification and commodification of women in publications, advertisements, and posters, a phenomenon that had attracted growing public concern and feminist advocacy through the 1970s and early 1980s. Its enactment represented a legislative recognition that the depiction of women in degrading and dehumanizing ways in visual media constituted a harm that required criminal law intervention, distinct from the general law of obscenity under the Indian Penal Code.

The definitional core of the statute, section 2(c), defines “indecent representation of women” as “the depiction in any manner of the figure of a woman; her form or body or any part thereof in such way as to have the effect of being indecent, or derogatory to, or denigrating, women, or is likely to deprave, corrupt or injure the public morality or morals.” Sections 3 and 4 operationalize this definition by prohibiting advertisements containing indecent representation and prohibiting the publication, sale, hire, distribution, or circulation of material containing such representation.¹⁹ Section 6 provides the penalty structure: for a first offence, imprisonment up to two years and a fine up to two thousand rupees; for a repeat offence, imprisonment of six months to five years and a fine of ten thousand rupees to one lakh rupees.²⁰

The Act served an important normative function in its time. It legally anchored “dignity” as a component of women's rights in the statutory framework, going beyond the general obscenity standard under the IPC to create a gender-specific prohibition that recognized women as the particular class of victims of objectifying media representation. Women's organizations and civil society groups used IRWA's remedy provisions to contest degrading portrayals in print and visual advertising, and the Act contributed to the broader legal consciousness that the commodification of women's bodies in commercial media was a legally cognizable harm. The statute's normative significance, its articulation of women's dignity as a protected value distinct from public morality in the abstract, remains valuable even as its operational utility has diminished.

B. The Digital Disjunction

The central problem confronting IRWA in the contemporary era is one of technological

¹⁸ Indecent Representation of Women (Prohibition) Act § 2(c) (1986) (India).

¹⁹ *Id.* §§ 3–4.

²⁰ *Id.* § 6.

mismatch. The statute's text and legislative history are anchored in print and traditional visual advertising. It does not speak the language of "electronic form," "computer resources," "social media platforms," "end-to-end encryption," "cloud storage," "user-generated content," or "algorithmic amplification." The cyberspace harms that overwhelmingly affect women today, image morphing, non-consensual intimate image sharing, deepfake pornography, cyberstalking, sextortion, misogynistic trolling, and coordinated online harassment campaigns, did not exist when IRWA was drafted and could not have been contemplated by its framers.

As Halder observed in 2013, the IRWA must be "harmoniously interpreted" with the IT Act to have any purchase in digital contexts, but this harmonious interpretation itself is uncertain and contested because there is no textual basis within IRWA to extend its reach to internet-mediated content.²¹ The Act does not define or reference "electronic form," "computer" or "computer network," "intermediary," or any of the technological concepts that are central to the IT Act's regulatory apparatus. Attempting to apply IRWA's provisions, designed for print publishers, advertisers, and physical distributors, to social media platforms, encrypted messaging applications, or AI-generated content stretches the statutory text beyond its reasonable interpretive limits and raises concerns about the rule of law and the principle of legality in criminal law.

C. The Failed Amendment and Its Significance

The Indecent Representation of Women (Prohibition) Amendment Bill, 2012, was introduced in Rajya Sabha in December 2012 to address the very gap analysed in this paper. The Bill sought to extend IRWA's scope to the internet, satellite communication, over-the-top (OTT) services, and electronic media, and to incorporate the concept of "electronic form" from the IT Act into IRWA's definitional framework. The Ministry of Women and Child Development further proposed in 2018 that IRWA be expanded to cover OTT platforms and messaging services, signalling continued executive recognition of the statute's inadequacy.²²

However, the Bill was withdrawn from Rajya Sabha on 26 July 2021 without being passed. This withdrawal represents a missed legislative opportunity of the first order. Had the 2012 Amendment been enacted, IRWA would today possess the textual basis to address internet-

²¹ Halder, *supra* note 6, at 193–94.

²² Press Information Bureau, WCD Proposes Amendments to Widen Scope of Indecent Representation of Women Act (June 4, 2018), <https://www.pib.gov.in/PressReleasePage.aspx?PRID=1534316>.

mediated indecent representation, and the enforcement trajectory documented in this paper might have been significantly different. The withdrawal is the structural explanation for IRWA's current technological obsolescence: it confirms that the legislative branch was aware of the problem, proposed a solution, and ultimately failed to act, leaving the statute frozen in its 1986 form while the digital landscape evolved beyond recognition.

IV. CYBERCRIME AGAINST WOMEN IN MAHARASHTRA: EMPIRICAL ANALYSIS

A. Macro-Level Trends: Maharashtra in the National Picture

Maharashtra has consistently been among the states with the highest rates of cybercrime registration in India. The data in Table 1, compiled from NCRB's *Crime in India* reports for 2019 through 2023, documents the trajectory of total cybercrime registrations in Maharashtra against the national total.²³

Table 1: Cyber Crimes Registered in Maharashtra vs. National Total (NCRB Data, 2019–2023)

Year	Maharashtra Registrations	% Change (YoY)	National Total	Maharashtra's Share
2019	4,967	,	44,735	~11.1%
2020	5,496	+10.6%	50,035	~11.0%
2021	5,562	+1.2%	52,974	~10.5%
2022	8,249	+48.3%	65,893	~12.5%
2023	8,103	–1.8%	86,420	~9.4%

Source: NCRB, Crime in India (2019–2023).

The data reveals a sustained and dramatic increase in cybercrime registrations in Maharashtra: from 4,967 in 2019 to 8,103 in 2023, a 63 per cent increase over five years. The most significant

²³ National Crime Records Bureau, *Crime in India* 2019, 2020, 2021, 2022, 2023 (Annual Reports) (India).

single-year spike occurred in 2022, when registrations increased by 48.3 per cent, reflecting the post-COVID surge in digital engagement and social media usage that accelerated pre-existing trends. Maharashtra consistently accounts for approximately 9 to 12.5 per cent of national cybercrime figures, a disproportionate concentration for a single state, reflecting its urbanization levels, internet penetration rates, and comparatively active reporting infrastructure. The marginal decline of 1.8 per cent in 2023 does not reflect a reduction in offences; it is more plausibly attributed to reporting fatigue, continued underreporting, and the low FIR-conversion rate noted in institutional assessments, including the Parliamentary Committee Report.

B. City-Wise Distribution: Urban Concentration of Cyber Harm

The city-wise data further reinforces the urban concentration of cyber-enabled gender-based violence in Maharashtra. Table 2 presents available and estimated figures for the principal cities.

Table 2: City-Wise Cyber Complaints by Women in Maharashtra (2021–2023)

City	2021	2022	2023	Trend
Mumbai	~4,500+ (est.)	4,724	4,131	Slight decline (likely underreporting)
Pune	225	357	487	Strong increase (+116% since 2021)
Nagpur	~300 (est.)	~400 (est.)	~500 (est.)	Gradual rise
Thane	~600–800 (est.)	~900 (est.)	~1,000 (est.)	Increasing trend
Nashik	~200–300 (est.)	~350 (est.)	~400 (est.)	Moderate rise
Aurangabad (CSN)	~150–250 (est.)	~300 (est.)	~350 (est.)	Emerging growth

Source: NCRB City-wise data; estimated figures reflect authors' interpolation from available

NCRB district data where exact city-level figures are not separately published.

Mumbai remains the primary hotspot for cyber complaints by women, unsurprising given the city's internet penetration rates, population density, and the concentration of digital infrastructure. Pune's 116 per cent increase in three years is the most significant trend in the data, consistent with the city's rapid digital growth and expanding young professional demographic. The gradual rises in Nagpur, Thane, Nashik, and Aurangabad (Chhatrapati Sambhajinagar) reflect expanding internet access across second and third-tier cities and, importantly, growing awareness of reporting channels including the NCRP portal. Across all cities, complaints are predominantly channelled through IT Act and BNS provisions rather than IRWA, a pattern that the empirical analysis in Part V further confirms.

C. The Underreporting Dimension

Underreporting remains a structural challenge that contextualizes all of the data presented above. Many victims of cyber-enabled gender-based violence are deterred from reporting by social stigma, ignorance of legal remedies, police apathy, and the risk of secondary victimization, the phenomenon whereby the reporting process itself inflicts further harm on the complainant. The NORC/ICRW report finds that the IT Act's "law enforcement and puritanical undertones" often lead women and marginalized communities to choose not to report their abuse, resulting in a systematic undercount of the true incidence of online gender-based violence.²⁴

The National Cyber Crime Reporting Portal (NCRP) provides an additional data source that illustrates the scale of the problem. Data from a written reply in Rajya Sabha shows that complaints of cybercrimes against women reached 76,657 in 2025, a 28,322-case increase from 2024, with sexually obscene material accounting for 37,743 complaints, the single largest category.²⁵ These figures represent only the complaints that were formally registered through the portal; the real victimization figures are almost certainly substantially higher. The underreporting dimension does not diminish the empirical significance of the trends documented above, rather, it suggests that the recorded data understates the true scale of the

²⁴ NORC/ICRW, *supra* note 11, at 5.

²⁵ Ministry of Home Affairs, Written Reply in Rajya Sabha (Mar. 2026) (India), reported in *Cybercrime Against Women Jumps to 76,657 in 2025*, The Telegraph India (Mar. 18, 2026), <https://www.telegraphindia.com/india/cybercrime-against-women-jumps-to-76657-in-2025-obscene-content-tops-complaints-says-government/cid/2152003>.

problem and, consequently, understates the inadequacy of IRWA's contribution to addressing it.

V. IRWA'S OPERATIONAL DECLINE: THE EMPIRICAL COMPARISON WITH IT ACT

A. The National Trajectory: IRWA Cases 2010–2021

The empirical record demonstrates that IRWA's use has dwindled to near-extinction even as online gender-based abuse has expanded exponentially. Press Information Bureau data based on NCRB records shows a dramatic national trajectory: 895 cases under IRWA in 2010, 453 in 2011, 141 in 2012, 362 in 2013, and a mere 47 in 2014, showing not merely a low baseline but a collapse into double digits by 2014.²⁶ This decline occurred precisely during the period when internet penetration in India was accelerating and social media platforms were achieving mass adoption, suggesting that the statute was unable to adapt to the changing technological environment in which gender-based visual harm was increasingly perpetrated.

In Maharashtra, the decline was even more dramatic. Cases registered under IRWA declined to zero consistently from 2018 to 2021. This is the most striking empirical finding of this paper: Maharashtra, India's most urbanized state, which simultaneously records some of the highest cybercrime figures in the country, registered zero IRWA cases in a four-year period. The complete absence of IRWA registrations in a state with thousands of cybercrime complaints strongly supports the hypothesis that IRWA has been operationally displaced by the IT Act as the statutory vehicle of choice for law enforcement agencies dealing with online obscenity and indecent content involving women.

Table 5: State/UT-wise Cases Registered (CR) and Persons Convicted (PCV) under the Indecent Representation of Women (Prohibition) Act, 1986 (2018–2021)

Sl. No.	State/UT	2018 CR	2018 PCV	2019 CR	2019 PCV	2020 CR	2020 PCV	2021 CR	2021 PCV
1	Andhra Pradesh	0	0	0	0	0	0	0	0
2	Arunachal Pradesh	0	0	0	0	0	0	0	0
3	Assam	0	0	0	0	0	0	0	0
4	Bihar	0	0	1	0	0	0	0	0
5	Chhattisgarh	1	0	0	0	0	0	1	0

²⁶ Press Information Bureau, Ministry of Women & Child Development, Written Replies on IRWA Cases (2015) (India).

Sl. No.	State/UT	2018 CR	2018 PCV	2019 CR	2019 PCV	2020 CR	2020 PCV	2021 CR	2021 PCV
6	Goa	0	0	0	0	0	0	0	0
7	Gujarat	0	0	0	0	2	0	0	0
8	Haryana	0	0	0	0	0	0	0	0
9	Himachal Pradesh	0	0	0	0	0	0	0	0
10	Jharkhand	0	0	0	0	0	0	8	0
11	Karnataka	1	0	0	0	1	0	1	0
12	Kerala	1	2	7	0	3	12	2	0
13	Madhya Pradesh	0	0	0	0	0	0	0	0
14	Maharashtra	1	0	0	0	0	0	0	0
15	Manipur	0	0	0	0	0	0	1	0
16	Meghalaya	0	0	0	0	0	0	0	0
17	Mizoram	0	0	0	0	0	0	0	0
18	Nagaland	0	0	0	0	0	0	0	0
19	Odisha	3	0	6	0	3	0	3	0
20	Punjab	1	0	1	0	0	0	0	0
21	Rajasthan	7	7	5	6	0	3	6	5
22	Sikkim	0	0	0	0	0	0	0	0
23	Tamil Nadu	4	0	2	0	3	0	1	0
24	Telangana	0	0	0	0	0	0	0	0
25	Tripura	0	0	0	0	0	0	1	0
26	Uttar Pradesh	3	0	1	0	0	0	0	0
27	Uttarakhand	0	0	0	0	0	0	0	0
28	West Bengal	0	0	1	0	0	0	4	0
	TOTAL (States)	22	9	24	6	12	15	28	5
29	Andaman & Nicobar Is.	0	0	0	0	0	0	0	0
30	Chandigarh	0	1	0	0	0	0	0	0
31	Dadra & Nagar Haveli	0	0	0	0	0	0	0	0
32	Delhi	0	0	0	1	0	0	0	0
33	Jammu & Kashmir	0	0	0	0	0	0	0	0
34	Ladakh	NA	NA	NA	NA	0	0	0	0
35	Lakshadweep	0	0	0	0	0	0	0	0
36	Puducherry	0	0	0	0	0	0	0	0
	TOTAL (UTs)	0	1	0	1	0	0	0	0
	GRAND TOTAL	22	10	24	7	12	15	28	5

Source: data.gov.in, “State/UT-wise Cases Registered (CR) and Persons Convicted (PCV) under the Indecent Representation of Women (Prohibition) Act, 1986 from 2018 to 2021.” National Crime Records Bureau (NCRB), Ministry of Home Affairs, Government of India.

The data in Table 5, provides definitive empirical corroboration for the central finding of this

paper. The dataset reveals that Maharashtra registered only one (1) case under the IRWA 1986 in 2018, recording zero convictions. Critically, Maharashtra registered zero cases under IRWA in every subsequent year, 2019, 2020, and 2021, with correspondingly zero convictions. This four-year pattern of absolute non-invocation, in a state that simultaneously recorded 5,496 cybercrime cases in 2020 and 5,562 in 2021 (Table 1), is not a statistical anomaly. It is the direct and measurable consequence of IRWA's pre-digital architecture: enforcement agencies confronted with cyber-enabled gender-based harm have no workable basis under IRWA's text to register complaints and have consistently defaulted to the Information Technology Act, 2000 and cognate provisions of the IPC / BNS. At the national level, the data further confirms that the total number of cases registered under IRWA across all States and UTs declined sharply: from 22 cases (States) + 0 (UTs) = 22 total in 2018, to 24 in 2019, then collapsing to only 12 cases in 2020, the lowest figure recorded in the dataset, before recovering marginally to 28 cases in 2021, driven almost entirely by outlier registrations in Jharkhand (8 cases) and Rajasthan (6 cases). Conviction data is equally instructive: zero persons were convicted under IRWA in Maharashtra in any of the four years covered by this dataset. Nationally, the highest conviction figure was only 15 in 2020, itself an anomaly driven by Kerala's 12 convictions in that year. The near-total absence of IRWA enforcement across India's most urbanized and digitally advanced state across four consecutive years is the empirical foundation upon which this paper's reform argument rests: the statute is not merely theoretically obsolete, it has ceased to function as an operational instrument of legal protection for women in cyberspace.

B. Contrast with IT Act Usage

Table 3 presents a comparative picture of IRWA case registrations against IT Act provisions for obscene and sexually explicit electronic content, drawing on PIB data, NCRB reports, and parliamentary replies.

Table 3: IRWA Cases vs. IT Act Section 67/67A Cases, National Comparison

Year / Category	Statute	No. of Cases / Complaints
2010	IRWA (All India)	895
2011	IRWA (All India)	453
2012	IRWA (All India)	141
2013	IRWA (All India)	362
2014	IRWA (All India)	47

2013	IT Act ss 67–67C (All India)	1,203
2014	IT Act ss 67–67C (All India)	758
2015	IT Act ss 67–67C (All India)	816
2014	Insult to modesty (within IT Act)	599
2015	Insult to modesty (within IT Act)	606
2021	Total Cybercrime (All India, NCRB)	52,974
2022	Total Cybercrime (All India, NCRB)	65,893
2023	Total Cybercrime (All India, NCRB)	86,420
2021	Maharashtra Cybercrime (NCRB)	5,562
2022	Maharashtra Cybercrime (NCRB)	8,249
2023	Maharashtra Cybercrime (NCRB)	8,103

Sources: PIB press releases based on NCRB data; NCRB Crime in India (2021–2023); Lok Sabha written replies.

The divergence between the two statutes is stark and instructive. While IRWA cases collapsed from 895 in 2010 to 47 in 2014 nationwide, IT Act cyber-obscenity cases under sections 67 to 67C numbered 1,203 in 2013 alone, representing approximately twenty-five times the scale of IRWA usage in that year. Within the IT Act category, cases specifically involving insult to the modesty of women numbered 599 in 2014 and 606 in 2015, each figure exceeding IRWA's total national caseload by an order of magnitude. By 2023, the total national cybercrime caseload stands at 86,420, of which Maharashtra alone contributes 8,103 cases, all prosecuted under IT Act and BNS provisions. A Lok Sabha reply on harassment of women on social media confirmed that 97 complaints of online trolling and harassment received by the Ministry of Women and Child Development were channelled through IT Act and IPC mechanisms, not IRWA.²⁷

²⁷ Lok Sabha, Written Reply on Harassment of Women on Social Media (2015) (India).

C. Doctrinal Explanation for the Divergence

From a doctrinal standpoint, the divergence between IRWA and the IT Act in digital enforcement contexts reflects the fundamentally different legal designs of the two statutes. IRWA is gender-specific and content-focused: it articulates a standard of women's dignity as a protected value and prohibits specific forms of visual representation that degrade that dignity. However, its text and legislative history are anchored in print media and traditional visual advertising, it does not possess the technological vocabulary necessary to regulate electronic content. The IT Act, by contrast, is gender-neutral but technology-specific: it speaks the language of "electronic form," "computer resources," "intermediary," and "due diligence," and its provisions on obscene and sexually explicit electronic content under sections 67 and 67A are directly applicable to internet-mediated harms.

The result of this doctrinal asymmetry is that IRWA functions as an important normative statement, it articulates the value of women's dignity in visual representation, but has limited operational role in contemporary cyber-law enforcement. The IT Act has become the primary statutory vehicle for cyber-violence prosecutions not because it is more attentive to women's dignity (it is not, it is gender-neutral) but because it possesses the technological specificity that law enforcement agencies require to investigate, charge, and prosecute digital offences. This displacement of IRWA by the IT Act in practice represents a loss of the gender-specific normative framework that IRWA uniquely provides, a loss that legislative reform must address.

VI. PUNISHMENTS: A COMPARATIVE STATUTORY ANALYSIS

A. Information Technology Act, 2000

Sections 67 and 67A of the IT Act are the most commonly applied provisions in cybercrime complaints by women involving obscene or sexually explicit electronic content.²⁸ Section 67 addresses the publication or transmission of obscene material in electronic form and prescribes: for a first offence, imprisonment up to three years and a fine up to five lakh rupees; for a repeat offence, imprisonment up to five years and a fine up to ten lakh rupees. Section 67A addresses the publication or transmission of material containing sexually explicit acts or conduct in electronic form and prescribes: for a first offence, imprisonment up to five years and a fine up to ten lakh rupees; for a repeat offence, imprisonment up to seven years and a fine up to ten

²⁸ Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, §§ 67, 67A (India).

lakh rupees.

Two additional provisions are frequently invoked. Section 66E addresses the violation of privacy through the intentional capture, publication, or transmission of images of a person's private area without consent, prescribing imprisonment up to three years and a fine up to two lakh rupees. Section 66D addresses cheating by personation using a computer resource, prescribing imprisonment up to three years and a fine up to one lakh rupees.

B. Bharatiya Nyaya Sanhita, 2023

A critical omission in much existing scholarship on cybercrime against women, including the Gurjalwar and Dixit paper, is the failure to acknowledge that the Indian Penal Code, 1860, was replaced by the Bharatiya Nyaya Sanhita, 2023 (BNS), effective 1 July 2024.²⁹ Any contemporary analysis of the enforcement framework must refer to BNS provisions rather than IPC provisions. The relevant BNS provisions include the following.

Section 292 of the BNS addresses obscenity and prescribes: for a first offence, imprisonment up to two years and a fine up to two thousand rupees; for a repeat offence, imprisonment up to five years and a fine up to five thousand rupees. This provision replaces the former section 292 of the IPC. Section 79 of the BNS addresses any word, gesture, or act intended to insult the modesty of a woman, prescribing imprisonment up to three years and a fine. This replaces the former section 509 of the IPC.

Section 78 of the BNS addresses stalking, including cyberstalking, and prescribes: for a first offence, imprisonment up to three years and a fine; for a repeat offence, imprisonment up to five years and a fine. This provision replaces the former section 354D of the IPC. Crucially, section 78 of the BNS explicitly includes the monitoring of a woman's use of "the internet, e-mail or any other form of electronic communication" within the statutory definition of stalking, achieving greater technological specificity than its predecessor and demonstrating that the legislature is capable of incorporating digital concepts into criminal law provisions when it chooses to do so.

²⁹ Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, 2023, §§ 78, 79, 292, (effective July 1, 2024).

C. IRWA, 1986, Section 6

Section 6 of IRWA provides the penalty structure for offences under the Act: for a first offence, imprisonment up to two years and a fine up to two thousand rupees; for a repeat offence, imprisonment of six months to five years and a fine of ten thousand rupees to one lakh rupees.³⁰ These penalties were set in 1986 and have never been revised, notwithstanding the fundamental transformation in the nature and scale of harms that the statute purports to address.

D. Comparative Table

Table 4: Comparative Punishment Framework, IT Act, BNS, and IRWA

Offence Category	Statute & Provision	First Offence	Repeat Offence
Obscene electronic content	IT Act s 67	3 yrs + ₹5 lakh	5 yrs + ₹10 lakh
Sexually explicit electronic content	IT Act s 67A	5 yrs + ₹10 lakh	7 yrs + ₹10 lakh
Privacy violation (images)	IT Act s 66E	3 yrs + ₹2 lakh	
Obscenity (general)	BNS s 292	2 yrs + ₹2,000	5 yrs + ₹5,000
Insult to modesty of woman	BNS s 79	3 yrs + fine	
Cyberstalking	BNS s 78	3 yrs + fine	5 yrs + fine
Indecent representation (general)	IRWA s 6	2 yrs + ₹2,000	6 mths–5 yrs + ₹10,000–₹1 lakh

Sources: IT Act (2000); BNS (2023); IRWA (1986).

³⁰ Indecent Representation of Women (Prohibition) Act § 6 (1986).

E. Analysis

The comparative table reveals a clear hierarchy of deterrence. The IT Act provides the harshest sanctions for digital offences, reflecting the legislative recognition that digital harm operates at a scale and speed that traditional media cannot match: a single act of uploading sexually explicit content can reach thousands or millions of viewers within hours. The IT Act's fine structure, up to ten lakh rupees, reflects this contemporary reality. IRWA, by contrast, provides the least severe penalties in the framework, particularly the two thousand rupee maximum fine for first offences. This fine was set in 1986 and has never been revised despite decades of inflation and the fundamental transformation of the media landscape.

The deterrence failure is most acutely illustrated by a concrete scenario: a perpetrator who morphs intimate images of a woman and distributes them across social media platforms to tens of thousands of viewers faces a maximum fine of only two thousand rupees under IRWA, the same quantum as the fine under BNS section 292 for selling an obscene pamphlet to a handful of individuals. The disparity between the severity of the harm and the severity of the sanction is indefensible. This penalty inadequacy is not merely a theoretical concern: it constitutes a practical deterrence failure that empirically explains IRWA's displacement by the IT Act. Law enforcement agencies, when presented with complaints of online gender-based abuse, rationally prefer to charge under IT Act provisions that provide both the technological specificity and the deterrent penalty structure that the situation demands.

VII. THE DEEPPAKE DIMENSION AND THE IT AMENDMENT RULES 2026

A particularly acute manifestation of IRWA's doctrinal inadequacy is the emergence of deepfake technology as a primary vehicle for gender-based cyber abuse. Global data shows that approximately 96 to 98 per cent of deepfake videos online constitute non-consensual pornography, with virtually all victims being women.³¹ The volume of such content grew 464 per cent between 2022 and 2023, reflecting both the increasing accessibility of AI-powered face-swapping tools and the absence of effective legal deterrence. In India, the NCRP recorded a 118.4 per cent rise in online crimes against women between 2020 and 2024, with deepfakes constituting a growing subset. A 2025 RATI Foundation report found that 10 per cent of all calls to its online abuse helpline involved deepfakes or AI-manipulated sexual images,

³¹ Why India's New Synthetic Content Rules Are a Women's Rights Issue, Bar & Bench (Mar. 2, 2026), <https://www.barandbench.com/view-point/why-indias-new-synthetic-content-rules-are-a-womens-rights-issue>.

underscoring the rapid mainstreaming of this form of abuse.

IRWA's section 2(c) definition, "representation of a woman's figure, form, or body", arguably extends to AI-generated synthetic imagery insofar as it depicts a woman's likeness. A deepfake that superimposes a real woman's face onto a pornographic body is, in a literal sense, a "depiction of the figure of a woman" that is "indecent" and "derogatory." However, this interpretation has not been judicially tested, and the definitional anchor in "figure, form, or body" was not drafted with synthetic media in mind. The absence of any reference to AI-generated content, synthetic imagery, or computational manipulation in IRWA's text creates interpretive uncertainty that undermines the statute's utility as a basis for prosecution. The result is a constitutional and statutory vacuum: Article 21 of the Constitution protects the right to life and dignity but operates primarily vertically against State action, leaving private actors who create and weaponize synthetic intimate images largely outside constitutional scrutiny.³²

The IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, represent the most significant regulatory response to the deepfake crisis to date. Effective 20 February 2026, these Rules introduce several important obligations.³³ They establish a statutory definition of "synthetically generated information" (SGI), mandate prominent labelling of SGI content and permanent metadata embedding to enable identification and tracing, impose a two-hour takedown obligation on Significant Social Media Intermediaries (SSMIs) for non-consensual intimate synthetic imagery upon receipt of a complaint, and require the deployment of automated technical measures for the detection of synthetic content. These provisions represent a meaningful step forward in addressing platform-level responsibilities.

However, commentators have rightly noted that the 2026 Amendment Rules address intermediary obligations rather than individual criminal liability.³⁴ A social media platform may be compelled to remove deepfake content within two hours, but the individual who created and uploaded that content faces criminal liability only under the existing, and inadequate, statutory framework: IRWA (with its two thousand rupee fine), IT Act sections 67 and 67A

³² *AI-Generated Deepfakes and the Legal Vacuum in India*, IJRTI (Nov. 2025), <https://www.ijrti.org/papers/IJRTI2511099.pdf>.

³³ Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, *supra* note 16.

³⁴ Dr. Shradha Sharma, *Technology-Facilitated Gender-Based Violence in India: Cyberbullying, Deepfakes, and the Law*, Indian J.L. & Legal Rsch. (Feb. 27, 2026), <https://www.ijllr.com/post/technology-facilitated-gender-based-violence-in-india-cyberbullying-deepfakes-and-the-law>.

(which address obscenity and sexual explicitness generally but do not create a specific offence for synthetic intimate imagery), and BNS provisions of general application. A dedicated criminal offence for the creation and non-consensual distribution of synthetic intimate imagery, of the kind enacted in Australia's Criminal Code Amendment (Deepfake Sexual Material) Bill 2024 and the United Kingdom's Online Safety Act, remains absent from Indian law. This gap between regulatory and criminal frameworks constitutes the most pressing unaddressed dimension of the deepfake challenge.

VIII. CRITICAL ENGAGEMENT WITH PRIOR SCHOLARSHIP

The most directly comparable published work on IRWA in the target journal is Gurjalwar and Dixit's "Critical Analysis of the Indecent Representation of Women (Prohibition) Act, 1986 and Its Relation to Patriarchy," published in the Indian Journal of Law and Legal Research, Volume VII Issue I.³⁵ A critical reading of that paper reveals several significant methodological and factual deficiencies that the present paper is specifically designed to address.

First, there is a fundamental factual misstatement of IRWA's penalties. Gurjalwar and Dixit state that "[t]he punishment for violating this law includes imprisonment of up to three years and a fine of up to Rs. 2 lakhs. Repeat offenders could face imprisonment of up to five years and a fine of up to Rs. 5 lakhs." This is incorrect. Section 6 of IRWA prescribes a maximum of two years' imprisonment, not three, and a fine of two thousand rupees, not two lakh rupees, for first offences.³⁶ The figures stated by the authors exceed the actual statutory fine by a factor of one hundred. For a piece of legal scholarship analysing a specific statute, an error of this magnitude in stating the statute's core penalty provision is a fundamental deficiency.

Second, there is a citation to a non-existent provision. The paper states that "[t]he Act was amended in 2013 to broaden its scope" and that "Section 354E (now Section 74 in BNS)" was included to criminalise non-consensual dissemination of sexually explicit content. Section 354E does not exist in the Indian Penal Code, 1860, it was never enacted. The Criminal Law (Amendment) Act, 2013, introduced sections 354A, 354B, 354C, and 354D, but not section 354E.³⁷ The citation to a non-existent provision in a statutory analysis paper is a serious error

³⁵ Gurjalwar & Dixit, *supra* note 17.

³⁶ Indecent Representation of Women (Prohibition) Act, § 6, (1986).

³⁷ The Criminal Law (Amendment) Act, 2013, No. 13, Acts of Parliament, 2013, §§ 354A–354D.

of legal accuracy that could mislead readers relying on the paper for an understanding of the legal framework.

Third, there is a complete absence of empirical grounding. The paper makes no use of NCRB data, NCRP complaint figures, parliamentary records, or any other empirical source. It makes the normative claim that “the act has been successful in curbing the issue to a certain extent” without providing any quantitative or qualitative evidence to support this assertion. This claim is directly contradicted by the data analysed in this paper: IRWA cases collapsed nationally from 895 in 2010 to 47 in 2014 and to zero in Maharashtra from 2018 to 2021. A claim of success in the face of these figures cannot be sustained without an evidentiary basis, which the paper does not provide.

Fourth, there is a reliance on non-academic and methodologically inappropriate sources. The paper’s citation apparatus relies primarily on blog posts, including iPleaders, and a 1981 Ph.D. dissertation on male nudity in advertising to support claims about gender representation in contemporary Indian films.³⁸ The absence of peer-reviewed legal scholarship, NCRB data, or judicial decisions in the footnotes of a statutory analysis paper represents a methodological shortcoming that this paper deliberately corrects through its reliance on primary statutory texts, official government data, Supreme Court decisions, and peer-reviewed academic literature.

This critique is offered not to diminish the value of prior scholarship on IRWA, any contribution to the understanding of a neglected statute has merit, but to demonstrate that the literature remains underdeveloped on the empirical and contemporary enforcement dimensions of IRWA’s operation. The gap that this paper fills is precisely the gap that the Gurjalwar and Dixit paper exemplifies: the absence of rigorous, data-driven, state-specific analysis of IRWA’s effectiveness in the age of digital gender-based violence.

IX. REFORM PROPOSALS

A. Amending IRWA for the Digital Age

The most urgent reform required is a comprehensive digital amendment to IRWA that bridges the technological gap documented in this paper. Such an amendment should incorporate four

³⁸ John A. Welsch, *An Investigation of the Effects of Male Nudity in Advertising on Product Brand Recall* (1981) (unpublished Ph.D. dissertation, Iowa State University).

core elements. First, it should introduce a definition of “electronic form” into section 2 of the Act, aligned with the definition in section 2(1)(r) of the IT Act, to establish the textual basis for IRWA’s application to digital content. Second, it should extend the prohibitions in sections 3 and 4 explicitly to internet-mediated content, social media platforms, OTT services, messaging applications, and AI-generated synthetic imagery. Third, it should introduce a new section 2(ca) defining “non-consensual intimate digital content” to encompass morphed images, deepfakes, revenge pornography, and other forms of digitally-facilitated gender-based abuse. Fourth, it should substantially revise the section 6 penalty structure to bring fines and imprisonment terms in line with the IT Act’s deterrent framework, at minimum, aligning the first-offence fine with the five lakh rupee threshold under IT Act section 67. The Parliamentary Standing Committee’s recommendation for a “comprehensive and gender-sensitive cybercrime law” provides institutional backing for this reform direction.³⁹

B. Convergence Between IRWA, the IT Act, and the BNS

The current fragmented multi-statute framework, in which IRWA, the IT Act, and the BNS each address overlapping aspects of the same conduct without clear coordination mechanisms, creates confusion for law enforcement agencies and imposes disproportionate burdens on victims navigating multiple legal avenues. The reform model should not replace any existing statute but should create clear cross-references and a unified enforcement mechanism. Specifically, a joint enforcement protocol should be developed between IRWA enforcement authorities and cyber cells operating under the IT Act, enabling coordinated investigation and prosecution of cases that engage both statutes. Courts should receive binding judicial guidance, through Practice Directions or Supreme Court guidelines, on how IRWA interacts with sections 67 and 67A of the IT Act and sections 78 and 79 of the BNS, clarifying the circumstances in which charges under multiple statutes are appropriate and the standards for each. The National Cyber Crime Reporting Portal should be modified to record IRWA-specific complaints as a separate category, enabling evidence-based policy monitoring and ensuring that the statute’s enforcement trajectory can be tracked against IT Act and BNS registrations.

C. Addressing the Deepfake Gap

India requires a specific criminal offence for the creation and non-consensual distribution of

³⁹ Comm. on Empowerment of Women, *supra* note 15.

synthetic intimate imagery, modelled on Australia's Criminal Code Amendment (Deepfake Sexual Material) Bill 2024 and the United Kingdom's Online Safety Act. The IT Amendment Rules 2026 address platform obligations through takedown requirements and metadata labelling mandates, but they do not impose individual criminal liability on the creators and distributors of deepfake content, a gap that must be closed through primary legislation. An expanded IRWA section 2(c) definition covering AI-generated likenesses, combined with enhanced penalties in section 6 and a new specific offence within the IT Act targeting the creation and distribution of non-consensual synthetic intimate imagery, would provide the integrated framework needed to address this rapidly growing form of abuse.

D. Institutional and Enforcement Reforms

Beyond legislative reform, institutional and enforcement improvements are essential to translate statutory provisions into effective protection for women. Four specific reforms are proposed. First, dedicated gender-cyber cells should be established in all district-level police stations in Maharashtra, staffed with officers trained specifically in digital evidence collection, preservation of electronic records, and gender-sensitive investigation protocols that minimize the risk of secondary victimization. Second, mandatory FIR conversion timelines should be introduced: complaints under IRWA and the IT Act involving non-consensual intimate content should require FIR registration within twenty-four hours under a proposed Standard Operating Procedure, eliminating the discretion that currently enables police inaction.

Third, victim support units should be established, as recommended by the Parliamentary Standing Committee, connecting women who are victims of cybercrime to One Stop Centres for counselling, legal aid, and rehabilitation services. These units should be integrated with the NCRP portal to enable seamless referral from complaint registration to support services. Fourth, an annual "IRWA Enforcement Audit" should be instituted, a systematic data collection exercise conducted by the NCRB specifically tracking IRWA complaint registrations, FIR conversions, charge-sheets filed, and convictions secured, disaggregated by state and offence category. This audit would build the evidence base necessary for ongoing legislative review and ensure that the statute's enforcement trajectory is transparently monitored rather than permitted to decline silently into irrelevance.

X. CONCLUSION

The Indecent Representation of Women (Prohibition) Act, 1986, was a pioneering statute when

it was enacted. It anchored women's dignity in statutory law, created a gender-specific prohibition against the commodification of the female body in visual media, and provided a legal basis for challenging degrading representations in print and advertising. These were genuine normative achievements that deserve recognition. However, the central argument of this paper, supported by the empirical data analysed across Parts IV and V, is that IRWA is now operationally obsolete in the digital age. This is not merely a doctrinal claim: it is empirically demonstrated by the data. Maharashtra registered zero IRWA cases from 2018 to 2021, while cybercrime registrations in the same state rose from 4,967 in 2019 to 8,103 in 2023. Nationally, IRWA cases collapsed from 895 in 2010 to 47 in 2014, even as IT Act cyber-obscenity cases numbered in the thousands.

The three research questions posed in the Introduction are answered as follows. First, IRWA is not effective in addressing cybercrime against women, the empirical record confirms that the statute plays no operational role in Maharashtra's cybercrime enforcement landscape and a negligible role nationally. Second, Maharashtra shows rising and urban-concentrated cyber harm, with complaints predominantly prosecuted under IT Act provisions and BNS provisions rather than IRWA. Third, IRWA and the IT Act interact in a supplementary and inconsistent manner, producing a fragmented enforcement framework that lacks coordination mechanisms, unified reporting categories, or clear judicial guidance on how the two statutes apply to the same conduct. The research hypothesis is confirmed: IRWA is inadequate as a pre-technological statute, and major legislative reform is required.

The institutional landscape has begun to respond. The IT (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2026, introduce significant platform-level obligations for synthetic content. The Parliamentary Standing Committee's Fourth Report of March 2026 documents a 239 per cent increase in cybercrimes against women and recommends a comprehensive and gender-sensitive cybercrime law. These developments demonstrate that both the executive and the legislature have recognised the inadequacy of existing frameworks. The reform window is open, but it requires specific, focused action on IRWA: digital amendments, enhanced penalties, convergence mechanisms, and dedicated enforcement infrastructure.

Women's dignity in cyberspace cannot be protected by statutes that do not recognise cyberspace exists. An amended, digitally-aware IRWA, integrated with the IT Act and the

Bharatiya Nyaya Sanhita, equipped with deterrent penalties, and supported by trained enforcement agencies, would not only address the existing enforcement gaps documented in this paper but would restore the gender-specific normative vision that IRWA originally pioneered and that the IT Act, in its gender-neutral technological focus, cannot replicate. The original promise of the 1986 Act, that the law would protect women from the commodification of their bodies in visual media, remains unfulfilled in the domain where such commodification now overwhelmingly occurs. It is time to bring IRWA into the digital age.