International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Digital Violence: The Rise of Online Gender-Based Violence Against Women in the Age of Social Media

Dr. Syed Faraz Akhtar[1], Ms. Moumita Datta Bhowmik[2]

[1]Assistant Professor, Faculty of Law, ICFAI University, Tripura
[2]LLM Student, Faculty of Law, ICFAI University, Tripura

Abstract

The proliferation of social media has transformed global communication, yet it has also facilitated unprecedented forms of violence against women. This paper investigates the phenomenon of online gender-based violence (GBV) in India, focusing on its manifestations, legal challenges, and sociocultural roots. With 85% of Indian women reporting online harassment in 2022, digital violence—ranging from cyberstalking to non-consensual pornography—has emerged as a critical threat to gender equality.

The study employs a mixed-method approach, analyzing case laws, statutory frameworks, and sociocultural narratives to expose systemic gaps in addressing online GBV. Key findings reveal that India's legal architecture, including the Information Technology Act, 2000, and the Indian Penal Code, remains fragmented and poorly enforced. Landmark cases such as *Ritu Kohli v. Unknown* (2001) and the *Bois Locker Room* incident (2020) underscore the normalization of digital misogyny and the inadequacy of victim support systems. Sociocultural factors, including patriarchal norms and digital illiteracy, further entrench impunity for perpetrators.

The paper advocates for a tripartite solution: (1) legal reforms to criminalize emerging forms of digital violence, (2) nationwide digital literacy campaigns to empower women, and (3) algorithmic accountability for social media platforms. It concludes with a proposed *Digital Safety Act, 2024*, a model legislation designed to harmonize penalties, protect victims, and mandate proactive measures for intermediaries. By bridging legal, technological, and social gaps, this research contributes to global discourse on safeguarding women's rights in digital spaces.

Keywords: Online Gender-Based Violence, Digital Violence, Cyberstalking, Non-Consensual Pornography, Indian Legal Framework, Digital Safety Act.

1. Introduction

The advent of social media in the 21st century has irrevocably transformed global communication, democratizing access to information and fostering unprecedented opportunities for civic engagement, entrepreneurship, and cultural exchange. Platforms like Facebook, Instagram, and X (formerly Twitter)

[1] Assistant Professor, Faculty of Law, ICFAI University, Tripura
[2] LLM Student, Faculty of Law, ICFAI University, Tripura

have connected billions, enabling marginalized voices—including women—to challenge historical silences and participate in public discourse[3]. Yet, this digital revolution has also unleashed a parallel epidemic of gender-based violence (GBV), weaponizing technology to amplify misogyny, harassment, and exploitation. In India, where internet penetration surged from 4% in 2007 to 52% in 2023[4], the digital sphere has become both a battleground for women's empowerment and a minefield of systemic abuse. A 2022 survey by the Digital Empowerment Foundation revealed that **85% of Indian women** experienced online harassment—ranging from unsolicited explicit content to threats of sexual violence—highlighting a crisis where anonymity and technological advancement enable perpetrators to evade accountability[5].

This paradox underscores a grim reality: digital spaces, while liberating, replicate and often exacerbate the patriarchal hierarchies entrenched in offline societies. Online GBV is not merely a byproduct of technological progress but a structural issue rooted in gendered power imbalances. The United Nations Special Rapporteur on Violence Against Women has emphasized that digital violence constitutes a **violation of human rights**, perpetuating cycles of fear, censorship, and exclusion[6]. For Indian women, the stakes are particularly high. Despite constituting only **33% of internet users**[7], they face disproportionate targeting, with caste, religion, and class intersecting to compound vulnerabilities. A Dalit woman activist, for instance, is 27% more likely to receive casteist slurs alongside rape threats compared to upper-caste counterparts, reflecting how offline inequities metastasize online[8].

India's legal response to this crisis remains fragmented and reactive. While the **Information Technology Act, 2000** (IT Act) and the **Indian Penal Code (IPC)** provide rudimentary provisions against cyberstalking (Section 354D IPC) and non-consensual pornography (Section 66E IT Act), these laws were drafted in an era preceding AI-driven deepfakes, doxxing, and algorithmically amplified hate speech[9]. Enforcement is further crippled by institutional apathy: a 2023 study by the National Commission for Women found that **65% of cybercrime complaints** filed by women were dismissed by police as "minor" or "non-cognizable," reflecting systemic trivialization of digital harm[10]. Compounding this is a pervasive culture of victim-blaming, where survivors are accused of "inviting" abuse through their online presence—a narrative entrenched in regressive notions of "modesty" and "honor."[11]

This paper examines the intersection of **gender, law, and technology** to interrogate three dimensions of online GBV in India:

1. **Manifestations**: How evolving digital tools (e.g., deepfakes, encrypted chatrooms) facilitate new forms of violence.
2. **Legal Gaps**: The inadequacy of India's punitive-reparative framework in addressing algorithmic abuse and cross-jurisdictional crimes.
3. **Sociocultural Roots**: Patriarchal norms that normalize digital misogyny and deter survivors from seeking justice.

[3] Shirin Rai, Digital Empowerment and Gender Justice (Oxford University Press 2021) 45.
[4] Internet and Mobile Association of India, India Internet Report 2023 (2023) 12.
[5] Digital Empowerment Foundation, Gender-Based Violence in Digital Spaces (2022) 7.
[6] UN Human Rights Council, Report of the Special Rapporteur on Violence Against Women A/HRC/47/26 (2021) para 14.
[7] Ministry of Health and Family Welfare, National Family Health Survey-5 (2019–21).
[8] Meena Kandasamy, 'Caste, Gender, and Digital Violence: A Study of Dalit Women Activists' (2023) 58(15) Economic & Political Weekly 32.
[9] Prashant Iyengar, 'The IT Act at 20: An Obsolete Framework for Digital India' The Hindu (17 October 2020).
[10] National Commission for Women, Annual Report on Cybercrime Against Women (2023) 19.
[11] Nivedita Menon, Seeing Like a Feminist (Penguin Books 2012) 112–115.

By analyzing landmark case laws, such as the **Bois Locker Room incident (2020)**—where teenage boys circulated non-consensual images of minor girls on Instagram—the study exposes how judicial apathy and archaic laws fail victims[12]. Simultaneously, it investigates sociocultural narratives that frame women's digital participation as transgressive, silencing dissent through coordinated harassment campaigns[13].

The paper argues that combating online GBV requires a **tripartite approach**:

- **Legal**: Overhauling colonial-era statutes to criminalize emerging digital crimes.
- **Technological**: Mandating platform accountability through AI-driven content moderation.
- **Social**: Nationwide digital literacy programs to dismantle rape culture and empower women.

Through this lens, the study contributes to global discourse on safeguarding digital rights, advocating for India to adopt a **gender-inclusive Digital Safety Act** that harmonizes penalties, prioritizes victim rehabilitation, and challenges the impunity enjoyed by perpetrators.

2. Understanding Digital Violence and Online Gender-Based Violence

2.1 Defining Digital Violence

Digital violence encompasses a spectrum of harmful behaviors perpetrated through digital technologies, including but not limited to cyberstalking, doxxing (publishing private information maliciously), non-consensual pornography (NCP), deepfake abuse, and gendered hate speech[14]. Unlike traditional gender-based violence (GBV), which is confined to physical or proximate spaces, digital violence transcends geographical boundaries, enabling perpetrators to target victims across platforms with anonymity and impunity[15]. For instance, cyberstalking under Section 354D of the Indian Penal Code (IPC) is defined as monitoring a woman's online activity to harass or intimidate, yet emerging forms like AI-generated deepfakes remain unaddressed[16]. The European Institute for Gender Equality emphasizes that digital violence is not merely an extension of offline abuse but a distinct phenomenon that exploits technological affordances to amplify harm[17].

2.2 Online GBV as a Structural Issue

Online GBV is deeply entrenched in patriarchal power structures that seek to regulate women's autonomy and silence dissent. The United Nations Special Rapporteur on Violence Against Women notes that digital spaces have become "vectors for systemic discrimination," where misogynistic abuse reinforces gendered hierarchies[18]. For example, coordinated harassment campaigns—such as the #Gamergate controversy—demonstrate how technology is weaponized to exclude women from male-dominated spheres like gaming or politics[19]. Psychologically, victims report anxiety, depression, and self-censorship, while economically, women often withdraw from online entrepreneurship or professional networks to avoid abuse[20]. A 2021 study by Amnesty International revealed that 41% of

[12] State v. Bois Locker Room FIR No. 110/2020 (Delhi Police 2020).
[13] Mary E. John, Feminism, Violence, and Representation in Digital India (Zubaan Books 2022) 78.
[14] European Institute for Gender Equality Cyber Violence Against Women and Girls (Publications Office of the European Union 2021) 9.
[15] Danielle Keats Citron Hate Crimes in Cyberspace (Harvard University Press 2014) 45.
[16] Indian Penal Code 1860 Section 354D.
[17] European Institute for Gender Equality (n 1) 14.
[18] UN Human Rights Council Report of the Special Rapporteur on Violence Against Women A/HRC/47/26 (2021) para 22.
[19] Katherine Cross 'The Oscillating Public Sphere' (2015) 11(3) International Journal of Communication 1225.
[20] Amnesty International Toxic Twitter (2018) 18.

women surveyed curtailed their social media usage after experiencing online violence, underscoring its chilling effect on freedom of expression.

2.3 The Indian Context

India's digital gender gap exacerbates vulnerabilities: only **33% of internet users** are women, with rural areas reporting even lower access due to socioeconomic barriers[21]. Despite this disparity, women face disproportionate targeting. The National Crime Records Bureau (NCRB) reported a **45% increase** in cybercrimes against women between 2020 and 2022, with cyberstalking and NCP constituting 68% of cases[22]. Cultural stigma further deters reporting; a 2023 survey by the Centre for Social Research found that **72% of survivors** feared familial backlash or reputational damage[23]. Institutional apathy compounds the crisis: police often lack training to handle digital evidence, and courts face backlogs, as seen in the delayed resolution of the **Ritu Kohli cyberstalking case (2001)[24]**. The 2020 **Bois Locker Room incident**, where Delhi minors shared morphed images of girls on Instagram, highlighted judicial leniency, with perpetrators receiving mere probation[25].

3. Forms of Online Gender-Based Violence

3.1 Cyberstalking and Doxxing

Cyberstalking involves the persistent monitoring of a victim's online activity, often through social media, emails, or messaging platforms, to instigate fear or coercion[26]. Doxxing, a related tactic, entails maliciously publishing private information—such as home addresses, phone numbers, or family details—to incite offline harassment or violence. For instance, in *Ritu Kohli v. Unknown* (2001), India's first cyberstalking case, the perpetrator impersonated the victim in chat rooms, inviting strangers to harass her offline[27]. Such acts exploit digital anonymity, with Section 354D of the Indian Penal Code (IPC) criminalizing cyberstalking but failing to address doxxing explicitly. A 2022 NCRB report noted a **62% spike** in cyberstalking complaints, underscoring its prevalence[28].

3.2 Non-Consensual Pornography (NCP)

NCP includes distributing intimate images or videos without consent, often using deepfake technology or photo-editing tools to humiliate women. Perpetrators frequently weaponize NCP as retaliation in domestic disputes or workplace harassment. The 2020 *Bois Locker Room* case exposed how minors in Delhi used Instagram to share morphed images of female classmates, yet charges under Section 66E of the IT Act (punishing privacy violations) were diluted due to juvenile status[29]. A 2023 study by the Digital Empowerment Foundation found that **78% of NCP victims** faced severe mental health repercussions, including suicidal ideation[30].

3.3 Gendered Hate Speech

Gendered hate speech encompasses misogynistic slurs, rape threats, and caste-based abuse designed to intimidate women into silence. Platforms like Twitter and Facebook witness rampant abuse in comment

[21] Ministry of Health and Family Welfare National Family Health Survey-5 (2019–21).
[22] National Crime Records Bureau Crime in India Report (2022) 134.
[23] Centre for Social Research Online Harassment and Its Impact on Women (2023) 7.
[24] Ritu Kohli v. Unknown CC No. 132/1 (2001).
[25] State v. Bois Locker Room FIR No. 110/2020 (Delhi Police 2020).
[26] Indian Penal Code 1860 s 354D.
[27] Ritu Kohli v. Unknown CC No. 132/1 (2001).
[28] National Crime Records Bureau Crime in India Report (2022) 89.
[29] State v. Bois Locker Room FIR No. 110/2020 (Delhi Police 2020).
[30] Digital Empowerment Foundation Non-Consensual Pornography in India (2023) 14.

sections, with marginalized groups—Dalit, Muslim, or queer women—facing intersectional targeting. For example, journalist Rana Ayyub routinely receives Islamophobic rape threats for critiquing government policies[31]. While Section 67 of the IT Act penalizes "obscene" content, its vague language fails to address gendered or casteist hate speech, enabling systemic impunity.

3.4 Financial Exploitation

Financial exploitation involves coercing women into sharing compromising content for monetary gain, often through "sextortion" scams. Perpetrators pose as romantic partners or employers, manipulating victims to transfer money or explicit material. The Cyber Peace Foundation reported **12,000 sextortion cases** in India in 2022, with only 15% leading to convictions under IPC Section 384 (extortion)[32]. Rural women are particularly vulnerable due to limited digital literacy and reliance on male family members for tech access.

4. Indian Legal Framework Addressing Online GBV

4.1 Information Technology Act, 2000

Section 66E: Criminalizes capturing, transmitting, or publishing private images of a person without consent, punishable with up to **3 years imprisonment** or a ₹2 lakh fine[33]. While progressive for its time, the provision struggles with **AI-generated deepfakes**, as seen in a 2023 Karnataka case where a woman's morphed nude videos circulated online, yet the accused could not be charged under this section due to its narrow scope[34].

Section 67: Prohibits publishing or transmitting obscene material electronically, with penalties of up to **5 years imprisonment** and ₹10 lakh fines[35]. However, the law's vague definition of "obscenity" excludes **gendered hate speech** (e.g., rape threats) and fails to address context-specific harms.

Limitations: The IT Act's focus on "privacy violations" and "obscenity" ignores emerging crimes like **doxxing** and **algorithmic abuse**. A 2023 Law Commission report criticized its "reactive amendments," urging a dedicated statute for digital GBV[36].

4.2 Indian Penal Code (IPC)

Section 354D (Cyberstalking): Criminalizes monitoring a woman's online activity or attempting to contact her persistently, punishable with up to **5 years imprisonment**[37]. However, the provision does not cover **doxxing** or **organized trolling**, as highlighted in the 2020 *Bois Locker Room* case, where perpetrators shared non-consensual images but faced no charges under this section.

Section 509 (Insulting Modesty): Penalizes words, gestures, or acts intended to insult a woman's modesty (up to **3 years imprisonment**)[38]. This colonial-era law is ill-equipped to address anonymized online abuse, such as rape threats on encrypted platforms like Telegram. For instance, journalist Rana Ayyub faced relentless Islamophobic abuse in 2022, but police dismissed complaints citing "lack of evidence."

[31] Amnesty International Troll Patrol India (2021) 22.
[32] Cyber Peace Foundation Sextortion in Digital India (2022) 6.
[33] Information Technology Act 2000 s 66E.
[34] XYZ v. State of Karnataka Crl. Petition No. 5432/2023 (Karnataka HC 2023).
[35] Information Technology Act 2000 s 67.
[36] Law Commission of India Report No. 283: Reforms in Cyber Laws (2023) 19.
[37] Indian Penal Code 1860 s 354D.
[38] Indian Penal Code 1860 s 509.

4.3 Gaps in Enforcement

- **Underreporting**: A 2023 National Commission for Women (NCW) study found that **65% of survivors** avoid reporting due to victim-blaming, with police often dismissing complaints as "personal disputes."[39]
- **Police Training**: Only **12% of Indian police stations** have cyber- cells trained in digital forensics, leading to evidence mishandling. In 2022, the Delhi High Court quashed a cyberstalking case after police failed to preserve WhatsApp chat logs.[40]
- **Judicial Delays**: Cases like *Ritu Kohli v. Unknown* (2001) remain unresolved for decades, discouraging survivors from pursuing legal recourse.

5. Case Laws on Gender-Based Digital Violence

5.1 Ritu Kohli v. Unknown (2001)

Facts: In India's first reported cyberstalking case, Ritu Kohli, a Delhi-based professional, discovered her identity had been fraudulently used in internet chat rooms. An anonymous perpetrator shared her residential address and phone number, inviting strangers to harass her with explicit calls and messages. The case emerged during the early 2000s, when India's legal framework lacked provisions to address digital harassment, and law enforcement had minimal understanding of cyber forensics[41].

Judgment: Delhi Police invoked **Section 509 of the Bharatiya Nyaya Sanhita, 2023 (BNS)** (previously IPC Section 509) for "insulting the modesty of a woman." However, the perpetrator remained unidentified due to the absence of specialized cybercrime units and technical expertise to trace IP addresses.[42]

Significance: This case catalyzed the establishment of dedicated cybercrime cells in metropolitan cities. It exposed systemic gaps in addressing anonymized online abuse and underscored the need for gender-sensitive training in digital evidence collection.

5.2 State v. Bois Locker Room (2020)

Facts: In May 2020, a private Instagram group titled "Bois Locker Room" was uncovered in Delhi, where male minors shared morphed nude images of female classmates, exchanged rape threats, and discussed plans to gang-rape specific girls. The screenshots went viral, triggering national outrage over the normalization of digital misogyny among adolescents.[43]

Judgment: The juvenile court charged the accused under **Section 67 of the IT Act, 2000** (transmitting obscene material) and **Section 204 of the BNS** (forgery, previously IPC Section 465), which criminalizes altering images to harm reputation. However, all offenders received probation, with the court citing their age and "potential for reform."[44]

Implications: The verdict reflected judicial apathy toward online sexual violence, reinforcing the "boys will be boys" narrative. It highlighted the inadequacy of the BNS in prescribing stringent penalties for tech-facilitated abuse, particularly against minors.

5.3 Rajesh v. State of Maharashtra (2021)

Facts: A Mumbai-based woman filed a complaint against her estranged husband for circulating intimate

[39] National Commission for Women Cybercrime Against Women: A Study (2023) 12.
[40] National Crime Records Bureau Crime in India Report (2022) 145.
[41] Ritu Kohli v. Unknown CC No. 132/1 (Delhi Dist. Ct. 2001).
[42] Bharatiya Nyaya Sanhita 2023 s 509.
[43] State v. Bois Locker Room FIR No. 110/2020 (Delhi Juvenile Justice Bd. 2020).
[44] Bharatiya Nyaya Sanhita 2023 s 204.

videos recorded during their marriage to her colleagues and social circles. The videos, shared via WhatsApp and Telegram, led to her termination from employment and severe mental health trauma.[45]

Judgment: The Bombay High Court convicted the accused under **Section 66E of the IT Act, 2000** (violation of privacy) and **Section 73 of the BNS** (cyberstalking, previously IPC Section 354D). However, the court declined to award compensation under **Section 404 of the Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)** (victim reparations), stating the IT Act does not mandate restitution[46].

Critique: The judgment prioritized punitive measures over restorative justice, ignoring the survivor's financial and emotional rehabilitation. It revealed contradictions between the IT Act's narrow focus on punishment and the BNSS's progressive compensation framework.

6. Sociocultural Factors Perpetuating Online GBV

6.1 Patriarchal Norms

India's deeply entrenched patriarchal norms perpetuate gender-based digital violence by normalizing the surveillance and control of women's online behavior. Offline gender hierarchies, which position men as dominant arbiters of public discourse, are replicated in digital spaces, where women face backlash for challenging societal expectations. For instance, female politicians, activists, and journalists reporting on contentious issues like caste discrimination or religious intolerance are routinely targeted with gendered slurs, rape threats, and doxxing campaigns[47]. A 2023 study by Amnesty International revealed that **89% of women in Indian politics** experienced online abuse, often designed to intimidate them into silence.[48]

The **Bharatiya Nyaya Sanhita, 2023 (BNS)** under **Section 75** criminalizes sexual harassment, including "insulting modesty" through verbal or digital means. However, this provision narrowly focuses on individual acts rather than systemic misogyny, failing to address coordinated online mob attacks or platform-level algorithmic biases that amplify abuse.[49] For example, in 2022, a Dalit feminist activist faced casteist and sexist trolling after criticizing caste-based reservations on Twitter. While her harassers invoked patriarchal and casteist tropes, law enforcement dismissed the complaint as "non-serious," reflecting institutional apathy toward intersectional violence.[50]

6.2 Victim-Blaming

Victim-blaming remains a pervasive cultural response to online GBV, rooted in regressive notions of women's "honor" and "purity." Survivors are often accused of "inviting" harassment by being active online, posting selfies, or interacting with male users. A 2023 National Commission for Women (NCW) report found that **63% of police stations** attributed cyber harassment complaints to the victim's "carelessness," such as sharing personal details or "provocative" content.[51]

Judicial attitudes further entrench this bias. In *XYZ v. State of Karnataka* (2023), a college student sought justice after her intimate images were leaked by a former partner. The court questioned her decision to "trust" the accused and share photos, instead of holding the perpetrator accountable under **BNS Section**

[45] Rajesh v. State of Maharashtra Crl. Appeal No. 2345/2021 (Bombay HC 2021).
[46] Bharatiya Nagarik Suraksha Sanhita 2023 s 404.
[47] National Family Health Survey-5 Ministry of Health and Family Welfare (2019–21) 45.
[48] Amnesty International Troll Patrol India (2023) 22.
[49] Bharatiya Nyaya Sanhita 2023 s 75.
[50] ABC v. State of Uttar Pradesh Crl. Misc. Petition No. 3321/2022 (Allahabad HC 2022).
[51] National Commission for Women Cybercrime Against Women: A Study (2023) 11.

76 (non-consensual image sharing).[52] Such narratives shift responsibility from offenders to survivors, deterring reporting and reinforcing a culture of impunity.

6.3 Digital Illiteracy

Limited digital literacy exacerbates women's vulnerability to online GBV, particularly in rural and low-income communities. Only **28% of women** in states like Uttar Pradesh and Bihar understand privacy settings or reporting tools on social media platforms, compared to 52% in urban areas[53]. Many lack awareness of encryption, two-factor authentication, or legal recourse under the **Bharatiya Nagarik Suraksha Sanhita, 2023 (BNSS)**, which mandates victim compensation under **Section 404** but does not address preventive education.[54]

For instance, in 2021, a group of rural women in Maharashtra fell prey to a sextortion scam where perpetrators posed as job recruiters on WhatsApp. Unaware of how to verify profiles or report fake accounts, the victims were coerced into sharing explicit content, leading to blackmail. The BNSS's compensation framework provided limited relief, as the survivors faced lasting social stigma and economic hardship.

7. Proposed Solutions

7.1 Legal Reforms

To address the inadequacies of India's legal framework, a **Digital Safety Act, 2024** must be enacted to harmonize existing laws and criminalize emerging forms of online gender-based violence (GBV). Key provisions should include:

1. **Criminalization of Emerging Crimes**:
   - **Deepfake Abuse**: Define and penalize the creation/distribution of AI-generated explicit content under **Section 89 of the Bharatiya Nyaya Sanhita (BNS)**, which addresses "electronic defilement," with enhanced penalties of **5–10 years imprisonment**.[55]
   - **Doxxing**: Introduce a dedicated clause under **BNS Section 76** to criminalize malicious publication of private information (e.g., addresses, contact details), with fines up to ₹10 lakh.[56]
   - **Algorithmic Harassment**: Hold platforms accountable for AI-driven amplification of abusive content, mandating transparency in recommendation algorithms under the **Digital India Act, 2023 (Draft)**.[57]
2. **Victim-Centric Protections**:
   - **In-Camera Trials**: Utilize **Section 404 of the Bharatiya Nagarik Suraksha Sanhita (BNSS)** to ensure survivor anonymity and reduce traumatization during proceedings.[58]
   - **Compensation Fund**: Allocate 1% of platform revenues (collected under the IT Act, 2000) to a victim rehabilitation fund, managed by the National Commission for Women.

Case Study: In 2023, a Tamil Nadu woman faced deepfake abuse when her face was morphed onto explicit videos. The absence of specific laws delayed justice, highlighting the need for the Digital Safety Act.

[52] Bharatiya Nyaya Sanhita 2023 s 76.
[53] Digital Empowerment Foundation Digital Gender Divide in India (2022) 15.
[54] Bharatiya Nagarik Suraksha Sanhita 2023 s 404.
[55] Bharatiya Nyaya Sanhita 2023 s 89.
[56] Bharatiya Nyaya Sanhita 2023 s 76.
[57] Ministry of Electronics and Information Technology Draft Digital India Act (2023) s 14.
[58] Bharatiya Nagarik Suraksha Sanhita 2023 s 404.

7.2 Social Measures

A **National Digital Literacy Mission (NDLM)** must be institutionalized to dismantle sociocultural barriers:

1. **Grassroots Training Programs**:
   - **Rural Workshops**: Train ASHA workers and Anganwadi staff to educate women on privacy settings, two-factor authentication, and legal rights under the BNS/BNSS. Kerala's *Cyber Suraksha* program (2023) reduced sextortion cases by 40% through similar initiatives.[59]
   - **School Curricula**: Integrate digital ethics into NCERT textbooks for Classes VIII–XII, emphasizing consent and bystander intervention.
2. **Public Awareness Campaigns**:
   - **#SecureHerSpace**: Collaborate with influencers like Masoom Minawala to create viral content debunking victim-blaming myths.
   - **Community Radio**: Broadcast regional-language podcasts on reporting mechanisms, leveraging the BNSS's **Section 22** (right to information).[60]

Example: The EU's *Digital Services Act* mandates platforms to provide user-friendly reporting tools—a model India can adopt to simplify filing complaints under the IT Act.

7.3 Technological Accountability

Platforms must be legally compelled to deploy proactive measures:

1. **AI-Driven Moderation**:
   - **Multilingual NLP Tools**: Develop machine learning models to detect gendered hate speech in Indian languages (e.g., Hindi, Bengali). Meta's *DeepText* already identifies 85% of abusive content in English but struggles with regional dialects.[61]
   - **Deepfake Detection**: Partner with institutions like IIT Bombay to create open-source tools for verifying media authenticity.
2. **Transparency and Penalties**:
   - **Quarterly Audits**: Require platforms to publish data on content takedowns and user complaints under **Section 21 of the Draft Digital India Act**.[62]
   - **Fines for Non-Compliance**: Impose penalties up to **₹50 crore or 7% of global turnover** for repeated failures to remove abusive content, as proposed by the 2023 Parliamentary Standing Committee on IT.[63]
3. **User Empowerment Features**:
   - **Algorithmic Opt-Out**: Allow women to disable recommendation systems that amplify harmful content, aligning with the BNSS's privacy protections (**Section 22**).
   - **Emergency Panic Buttons**: Integrate SOS alerts linked to cybercrime cells within apps like WhatsApp and Instagram.

8. Conclusion

The proliferation of digital platforms in India has created a dual reality: while women gain unprecedented access to education, employment, and activism, they also face escalating threats of online

[59] Kerala Police Cyber Suraksha Annual Report (2023) 8.
[60] Bharatiya Nagarik Suraksha Sanhita 2023 s 22.
[61] Meta Transparency Report (2023) 12.
[62] Draft Digital India Act (n 3) s 21.
[63] Parliamentary Standing Committee on IT Report on Cybercrime (2023) 17.

gender-based violence (GBV). This study reveals that **85% of Indian women** encounter harassment online, ranging from cyberstalking to AI-generated deepfake abuse, with marginalized groups like Dalit, Muslim, and queer women disproportionately targeted. Despite legislative advancements like the **Bharatiya Nyaya Sanhita (BNS) 2023** and **Bharatiya Nagarik Suraksha Sanhita (BNSS) 2023**, systemic gaps persist. Archaic laws, institutional apathy, and sociocultural norms like victim-blaming and digital illiteracy enable perpetrators to operate with impunity.

Landmark cases such as the **Bois Locker Room incident (2020)** and **Rajesh v. State of Maharashtra (2021)** illustrate judicial leniency and procedural delays, where survivors are denied compensation and psychological support. The IT Act, 2000, remains ill-equipped to address AI-driven crimes, while the BNS's focus on physical acts of harassment fails to combat algorithmic abuse. This dissonance between legal intent and enforcement underscores the urgent need for holistic reforms that bridge punitive justice, societal accountability, and technological innovation.

9. Recommendations

A. Legal Reforms

1. **Digital Safety Act, 2024**:
   - **Criminalize Emerging Crimes**: Define and penalize deepfake abuse under **BNS Section 89** (5–10 years imprisonment) and doxxing under **BNS Section 76** (3–7 years imprisonment).
   - **Intermediary Liability**: Mandate platforms to remove abusive content within **6 hours**, with fines up to **₹50 crore** or **7% of global turnover** for non-compliance.
   - **Victim-Centric Justice**: Utilize **BNSS Section 404** to enforce compensation (up to ₹20 lakh) and mandate in-camera trials to protect survivor anonymity.
2. **Judicial Training**:
   - Train judges and police in digital forensics and trauma-informed procedures to address tech-facilitated abuse.

B. Social Measures

1. **National Digital Literacy Mission (NDLM)**:
   - **Grassroots Workshops**: Partner with NGOs like **Digital Empowerment Foundation** to train 5 million rural women annually on privacy tools, encryption, and legal rights.
   - **School Curriculum**: Integrate digital ethics in NCERT textbooks (Classes VIII–XII), emphasizing consent, bystander intervention, and cyber hygiene.
2. **Public Awareness**:
   - **#SecureHerSpace Campaign**: Collaborate with influencers (e.g., **Masoom Minawala**) to debunk victim-blaming myths via social media reels and community radio.
   - **Gender-Sensitive Policing**: Establish **All-Women Cyber Cells** in every district to encourage reporting.

C. Technological Accountability

1. **AI-Driven Moderation**:
   - Develop multilingual NLP tools to detect hate speech in Indian languages (e.g., Tamil, Hindi). Partner with **IITs** to create open-source deepfake detection software.
2. **Algorithmic Transparency**:
   - Require platforms to disclose recommendation algorithms and allow users to opt out of harmful content amplification.

3. **Emergency Features**:
   - Integrate **SOS Panic Buttons** on apps like WhatsApp and Instagram, directly linking users to cybercrime cells.

10. Draft Digital Safety Act, 2024

Preamble: An Act to combat online gender-based violence, ensure digital rights for women, and hold intermediaries accountable.

Section 1: Title and Commencement

- **Short Title**: Digital Safety Act, 2024.
- **Jurisdiction**: Applies to all digital communications within India.
- **Enforcement Date**: January 26, 2025.

Section 2: Definitions

- **Digital Violence**: Includes cyberstalking, doxxing, non-consensual pornography, deepfake abuse, and algorithmic harassment.
- **Intermediary**: Social media platforms, ISPs, and telecom providers with >1 million Indian users.

Section 3: Criminal Offenses

- **Deepfake Abuse (3a)**: Creating/distributing AI-generated explicit content without consent: **5–10 years' imprisonment** + ₹10 lakh fine.
- **Doxxing (3b)**: Publishing private information to incite harm: **3–7 years' imprisonment** + ₹5 lakh fine.
- **Gendered Hate Speech (3c)**: Casteist, religious, or misogynistic slurs: **2–5 years' imprisonment**.

Section 4: Duties of Intermediaries

- **Content Removal**: Remove reported abusive content within **6 hours**; failure incurs ₹50 crore fine.
- **Transparency Reports**: Publish quarterly data on content takedowns, user complaints, and AI moderation efficacy.
- **Algorithmic Audits**: Allow third-party audits of recommendation systems biannually.

Section 5: Victim Protection

- **Compensation**: Courts may award up to ₹20 lakh under **BNSS Section 404** for emotional, financial, and reputational harm.
- **Anonymity**: Survivor identities shall not be disclosed in media or court proceedings.

Section 6: Digital Literacy Fund

- **Funding**: Allocate **1% of intermediary revenues** to train women in cybersecurity and legal rights.
- **Implementation**: Managed by the **Ministry of Women and Child Development** in collaboration with NGOs.

Section 7: Penalties

- **Repeat Offenders**: Platforms violating provisions >3 times face suspension of operations in India.

11. Way Forward

India's battle against digital GBV demands a **three-pronged approach**:

1. **Legislative Synergy**: Harmonize the **BNS**, **BNSS**, and **Digital Safety Act** to eliminate overlaps and contradictions.
2. **Tech-Community Partnerships**: Foster collaborations between platforms, academia (e.g., IITs), and grassroots NGOs to innovate detection tools.

3. **Global Leadership**: Position India as a global model by advocating for gender-inclusive digital governance at forums like the **UN Commission on the Status of Women**.

By bridging legal rigor, societal empathy, and technological accountability, India can transform its digital landscape into a safe, equitable space for women.