



# INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

VOLUME 3 ISSUE 1

Peer-reviewed, open-access, refereed journal

**IJLAR**

+91 70421 48991  
editor@ijlar.com  
www.ijlar.com

## **DISCLAIMER**

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

## **Introduction**

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

## **Preface**

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

## **Description**

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

# **“DIGITAL PATRIARCHY AND ONLINE GENDER-BASED VIOLENCE IN INDIA: A CRITICAL ANALYSIS OF LEGAL RESPONSES AND ENFORCEMENT GAPS”**

AUTHORED BY - MAHIMA SINGH

## **Abstract<sup>1</sup>**

The rapid expansion of digital technologies and social media platforms in India has created new spaces for expression, communication, and participation. However, alongside these opportunities, the digital sphere has also become a site for pervasive gender-based violence, disproportionately affecting women. Online harassment, cyberstalking, non-consensual dissemination of intimate images, and abusive trolling have emerged as significant challenges, reflecting the persistence of patriarchal norms in virtual environments—a phenomenon often described as “digital patriarchy.”

This paper critically examines the adequacy of India’s existing legal framework in addressing online gender-based violence. It analyses key statutory provisions, including the Information Technology Act, 2000, and relevant sections of the Indian Penal Code, to assess their effectiveness in combating emerging forms of cyber abuse. While these laws provide a foundational structure for legal redress, their application in practice remains inconsistent due to definitional ambiguities, procedural delays, and lack of awareness among enforcement agencies.

The study further explores the role of digital platforms as intermediaries, highlighting concerns related to content moderation, accountability, and algorithmic amplification of harmful content. It argues that the current regulatory approach places insufficient responsibility on platforms, thereby limiting the effectiveness of legal remedies available to victims. Additionally, the paper examines enforcement challenges such as underreporting, victim-blaming, jurisdictional complexities, and the absence of gender-sensitive policing.

---

<sup>1</sup> Ms Mahima Singh is PhD. Scholar at Ram Manohar Lohia National Law University, Lucknow

Through a comparative analysis of international practices, the research identifies best practices that can inform India's approach to regulating online harms. The paper ultimately argues for a more robust and victim-centric legal framework that integrates technological, legal, and policy measures. It recommends clearer legal definitions, stronger platform accountability, capacity-building for law enforcement, and the development of specialised mechanisms to address online gender-based violence.

In conclusion, addressing digital patriarchy requires not only legal reform but also a broader socio-legal shift to ensure safe and equitable digital spaces for women in India.

### **Introduction: Rise of Digital Platforms and Gendered Harms in India**

The rapid proliferation of digital technologies in India has significantly transformed the social, economic, and cultural landscape. With increased internet penetration, affordable smartphones, and the widespread use of social media platforms, digital spaces have become central to communication, expression, and participation. Women, in particular, have increasingly engaged with these platforms for education, employment, activism, and social interaction. However, this digital empowerment has been accompanied by a parallel rise in gender-specific harms, reflecting the deep-rooted structural inequalities present in society.<sup>2</sup>

Online spaces, often perceived as neutral and democratizing, have instead replicated and, in many cases, intensified existing patriarchal norms. Women in India frequently face various forms of online gender-based violence, including cyberstalking, sexual harassment, non-consensual sharing of intimate images, and coordinated trolling. These forms of abuse not only violate individual dignity and privacy but also have a chilling effect on women's freedom of expression and participation in digital discourse.<sup>3</sup>

The concept of "digital patriarchy" captures this intersection between technology and entrenched gender hierarchies, highlighting how digital platforms can reinforce systemic discrimination.

---

<sup>2</sup> Catharine A MacKinnon, *Sex Equality* (Foundation Press 2001)

<sup>3</sup> Smriti Parsheera, 'Platform Regulation in India' (2018) *Indian Journal of Law and Technology* 1

Unlike traditional forms of violence, online abuse operates across borders, is often anonymous, and can be perpetuated at scale, making it more difficult to regulate and control. The psychological, social, and professional consequences for victims are significant, often leading to withdrawal from digital spaces altogether.<sup>4</sup>

In India, the legal framework addressing such harms is fragmented, relying on a combination of provisions under the Information Technology Act, 2000<sup>5</sup>, and the Indian Penal Code<sup>6</sup>. While these laws provide certain remedies, they were not originally designed to address the complexities of digital gender-based violence. As a result, gaps in legal interpretation, enforcement, and victim protection persist.

Against this backdrop, this paper seeks to critically examine the phenomenon of digital patriarchy and the effectiveness of India's legal response to online gender-based violence, with a view to identifying key challenges and proposing necessary reforms.<sup>7</sup>

## **2. Conceptual Framework: Understanding Digital Patriarchy and Online Gender-Based Violence**

The concept of “digital patriarchy” provides a critical lens through which the intersection of technology and gender inequality can be examined. While digital platforms are often portrayed as neutral spaces facilitating free expression and equal participation, they are, in reality, embedded within existing social structures that reflect and reproduce patriarchal norms. Digital patriarchy, therefore, refers to the continuation and amplification of gender-based discrimination, control, and marginalisation of women within online environments.<sup>8</sup>

Online gender-based violence (OGBV) is a key manifestation of digital patriarchy. It encompasses a wide range of harmful behaviours directed at individuals based on their gender, primarily

---

<sup>4</sup> Kimberlé Crenshaw, ‘Mapping the Margins’ in *Critical Race Theory* (New Press 1995).

<sup>5</sup> Information Technology Act 2000

<sup>6</sup> Indian Penal Code 1860.

<sup>7</sup> Martha C Nussbaum, *Women and Human Development* (Cambridge University Press 2000)

<sup>8</sup> Upendra Baxi, *The Future of Human Rights* (3rd edn, OUP 2008)

targeting women and marginalized groups. These behaviours include cyberstalking, online harassment, doxxing, non-consensual dissemination of intimate images, morphing of photographs, and coordinated trolling. Unlike offline violence, OGBV operates in a borderless, instantaneous, and often anonymous environment, which intensifies its impact and complicates legal regulation. A defining feature of OGBV is its scalability and persistence. Harmful content can be rapidly disseminated to large audiences and may remain accessible indefinitely, thereby prolonging the victim's trauma. Additionally, the anonymity afforded by digital platforms reduces accountability, enabling perpetrators to engage in abusive conduct with minimal fear of consequences. This creates a power imbalance, where victims are often silenced or forced to withdraw from online spaces.<sup>9</sup>

From a legal perspective, the conceptual challenge lies in categorising such conduct within existing frameworks. Traditional legal doctrines tend to distinguish between public and private harm, as well as physical and non-physical violence. However, online abuse often blurs these boundaries, combining elements of psychological harm, reputational damage, and invasion of privacy. As a result, existing legal categories may fail to adequately capture the seriousness and complexity of such conduct.

Furthermore, digital platforms themselves play a crucial role in shaping online interactions. Algorithmic amplification, content recommendation systems, and engagement-driven models may inadvertently promote harmful content, thereby reinforcing patterns of abuse. This raises important questions about platform responsibility and the extent to which intermediaries should be held accountable for user-generated content.<sup>10</sup>

Thus, understanding digital patriarchy and online gender-based violence requires a multidisciplinary approach that integrates legal, sociological, and technological perspectives, highlighting the need for more nuanced and adaptive regulatory frameworks.

---

<sup>9</sup> Justice Verma Committee, Report on Amendments to Criminal Law (2013).

<sup>10</sup> Danielle Keats Citron, 'Cyber Civil Rights' (2009) 89 Boston University Law Review 61.

## 2. Conceptual Framework: Understanding Digital Patriarchy and Online Gender-Based Violence

The concept of “digital patriarchy” provides a critical lens through which the intersection of technology and gender inequality can be examined. While digital platforms are often portrayed as neutral spaces facilitating free expression and equal participation, they are, in reality, embedded within existing social structures that reflect and reproduce patriarchal norms. Digital patriarchy, therefore, refers to the continuation and amplification of gender-based discrimination, control, and marginalisation of women within online environments.<sup>11</sup>

Online gender-based violence (OGBV) is a key manifestation of digital patriarchy. It encompasses a wide range of harmful behaviours directed at individuals based on their gender, primarily targeting women and marginalized groups. These behaviours include cyberstalking, online harassment, doxxing, non-consensual dissemination of intimate images, morphing of photographs, and coordinated trolling. Unlike offline violence, OGBV operates in a borderless, instantaneous, and often anonymous environment, which intensifies its impact and complicates legal regulation. A defining feature of OGBV is its scalability and persistence. Harmful content can be rapidly disseminated to large audiences and may remain accessible indefinitely, thereby prolonging the victim’s trauma. Additionally, the anonymity afforded by digital platforms reduces accountability, enabling perpetrators to engage in abusive conduct with minimal fear of consequences. This creates a power imbalance, where victims are often silenced or forced to withdraw from online spaces.<sup>12</sup>

From a legal perspective, the conceptual challenge lies in categorising such conduct within existing frameworks. Traditional legal doctrines tend to distinguish between public and private harm, as well as physical and non-physical violence. However, online abuse often blurs these boundaries, combining elements of psychological harm, reputational damage, and invasion of privacy. As a result, existing legal categories may fail to adequately capture the seriousness and complexity of such conduct.<sup>13</sup>

---

<sup>11</sup> Justice Verma Committee, Report on Amendments to Criminal Law (2013).

<sup>12</sup> Danielle Keats Citron, ‘Cyber Civil Rights’ (2009) 89 Boston University Law Review 61.

<sup>13</sup> Danielle Keats Citron, ‘Hate Crimes in Cyberspace’ (Harvard University Press 2014).

Furthermore, digital platforms themselves play a crucial role in shaping online interactions. Algorithmic amplification, content recommendation systems, and engagement-driven models may inadvertently promote harmful content, thereby reinforcing patterns of abuse. This raises important questions about platform responsibility and the extent to which intermediaries should be held accountable for user-generated content.

Thus, understanding digital patriarchy and online gender-based violence requires a multidisciplinary approach that integrates legal, sociological, and technological perspectives, highlighting the need for more nuanced and adaptive regulatory frameworks.<sup>14</sup>

### 3. Legal Framework in India: IT Act, IPC and Other Relevant Laws

The legal framework addressing online gender-based violence in India is primarily derived from a combination of provisions under the Information Technology Act, 2000<sup>15</sup> and the Indian Penal Code, 1860<sup>16</sup>(now BNS, 2023<sup>17</sup>) These laws, although not originally designed to specifically tackle digital gender-based harms, have been adapted over time to address emerging challenges in cyberspace. However, their fragmented nature often limits their effectiveness in providing comprehensive protection to victims.

Under the Information Technology Act, 2000, several provisions<sup>18</sup> are relevant in cases of online abuse. Section 66E<sup>19</sup> deals with the violation of privacy, penalising the capturing, publishing, or transmission of images of a person's private areas without consent. Section 67<sup>20</sup>, along with Sections 67A<sup>21</sup> and 67B<sup>22</sup>, addresses the publication or transmission of obscene and sexually explicit content in electronic form. Additionally, Section 69A<sup>23</sup> empowers the government to block public access to unlawful online content. While these provisions provide a legal basis for

---

<sup>14</sup> Mary Anne Franks, 'Unwilling Avatars' (2012) 20 Columbia Journal of Gender and Law 224.

<sup>15</sup> Information Technology Act 2000.

<sup>16</sup> Indian Penal Code 1860.

<sup>17</sup> Bharatiya Nyaya Sanhita 2023.

<sup>18</sup> Information Technology Act 2000

<sup>19</sup> Information Technology Act 2000, s 66E.

<sup>20</sup> Information Technology Act 2000, s 67.

<sup>21</sup> Information Technology Act 2000, s 67A.

<sup>22</sup> Information Technology Act 2000, s 67B.

<sup>23</sup> Information Technology Act 2000, s 69A.

regulating harmful digital content, their scope is often limited and subject to interpretational challenges.

The Bharatiya Nyaya Sanhita, 2023<sup>24</sup> supplements these provisions by criminalising various forms of harassment and abuse through updated and consolidated offences. Section 75<sup>25</sup> of the BNS addresses sexual harassment, covering acts such as unwelcome physical contact, demands for sexual favours, and sexually coloured remarks. Section 78<sup>26</sup> specifically deals with stalking, including monitoring a woman's online activities or repeatedly attempting to contact her despite clear disinterest, thereby explicitly recognising cyberstalking within its scope. Further, provisions relating to defamation and criminal intimidation are incorporated under the broader framework of offences against the human body and reputation. Additionally, Section 79<sup>27</sup> criminalises words, gestures, or acts intended to insult the modesty of a woman, which can be invoked in cases of online harassment and abusive digital conduct.

Despite the availability of these provisions, significant gaps remain. The laws do not explicitly recognise or define online gender-based violence as a distinct category, leading to inconsistent application and interpretation. Moreover, procedural challenges such as delays in investigation, lack of technical expertise among law enforcement agencies, and jurisdictional issues in cross-border cases hinder effective enforcement.

The role of intermediary liability, governed by Section 79 of the IT Act<sup>28</sup> and the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, is also crucial. While intermediaries are required to exercise due diligence and remove unlawful content upon notice, the extent of their accountability remains a subject of debate.

---

<sup>24</sup> Bharatiya Nyaya Sanhita 2023

<sup>25</sup> Bharatiya Nyaya Sanhita 2023, s 75.

<sup>26</sup> Bharatiya Nyaya Sanhita 2023, s 78.

<sup>27</sup> Bharatiya Nyaya Sanhita 2023, s 79.

<sup>28</sup> Information Technology Act 2000, s 79.

In sum, although India possesses a foundational legal framework to address online harms, it requires greater coherence, clarity, and adaptation to effectively tackle the evolving nature of digital gender-based violence.<sup>29</sup>

#### **4. Nature and Forms of Online Gender-Based Violence: Emerging Trends and Case Analysis**

Online gender-based violence (OGBV) in India manifests in diverse and evolving forms, reflecting both technological advancements and deeply embedded social inequalities. Unlike traditional forms of violence, OGBV is not confined by physical boundaries and often operates through anonymity, making it more pervasive and difficult to regulate. Understanding the various forms of such violence is essential for assessing the adequacy of legal responses and identifying enforcement gaps.

One of the most common forms of OGBV is cyber harassment, which includes abusive messages, threats, and persistent unwanted communication. Women, particularly those active in public life such as journalists, activists, and content creators, are frequently subjected to coordinated trolling campaigns. These campaigns often involve the use of derogatory language, rape threats, and character assassination, aimed at silencing women's voices and discouraging their participation in online discourse.<sup>30</sup>

Another significant form is cyberstalking, where perpetrators continuously monitor, contact, or attempt to control the victim's online activities. This may include tracking social media profiles, sending repeated messages, or using digital tools to surveil individuals. The psychological impact of such behaviour can be severe, leading to anxiety, fear, and withdrawal from digital platforms.<sup>31</sup> The non-consensual dissemination of intimate images, commonly referred to as "revenge porn," is also a growing concern in India. In such cases, private images or videos are shared without the consent of the individual, often with the intent to humiliate or blackmail. Advances in technology

---

<sup>29</sup> Danielle Keats Citron, 'Hate Crimes in Cyberspace' (Harvard University Press 2014).

<sup>30</sup> Mary Anne Franks, 'Unwilling Avatars' (2012) 20 Columbia Journal of Gender and Law 224.

<sup>31</sup> Ann Bartow, 'Internet Defamation as Profit Center' (2009) 32 Harvard Journal of Law & Gender 383.

have further exacerbated this issue through the use of image morphing and deepfake techniques, where manipulated content is created to falsely depict individuals in compromising situations.

Doxxing, which involves the public release of personal information such as addresses, phone numbers, and workplace details, is another form of online abuse that disproportionately targets women. This not only invades privacy but also exposes victims to offline risks, including physical harm. Additionally, impersonation and fake profiles are frequently used to damage reputations or engage in fraudulent activities.<sup>32</sup>

Recent trends indicate that algorithm-driven amplification on social media platforms can intensify the spread of abusive content, increasing its reach and impact. While Indian case law on OGBV is still developing, several reported instances demonstrate the growing recognition of such harms by courts and authorities. However, the absence of a unified legal approach continues to hinder consistent redressal.

Overall, the multifaceted nature of online gender-based violence highlights the urgent need for a comprehensive and adaptive legal framework capable of addressing both existing and emerging forms of digital harm.<sup>33</sup>

## **5. Challenges in Enforcement: Policing, Platform Accountability and Underreporting**

The enforcement of laws addressing online gender-based violence in India is fraught with multiple structural, procedural, and institutional challenges. Despite the existence of legal provisions under the Information Technology Act, 2000 and the BNS, their practical implementation remains inconsistent and often ineffective. This gap between law and enforcement significantly undermines the ability of victims to seek timely and meaningful redress.<sup>34</sup>

---

<sup>32</sup> Amanda Lenhart and others, 'Online Harassment' (2016) Pew Research Center Report.

<sup>33</sup> Ann Bartow, 'Internet Defamation as Profit Center' (2009) 32 Harvard Journal of Law & Gender 383.

<sup>34</sup> Information Technology Act 2000, & BNS, 2023.

One of the primary challenges lies in policing and investigative capacity. Law enforcement agencies frequently lack the necessary technical expertise and training required to handle cyber-related offences. Digital evidence collection, tracing anonymous perpetrators, and navigating encrypted communication channels require specialised skills that are not uniformly available across police departments. Additionally, delays in registering First Information Reports (FIRs) and a lack of sensitivity in dealing with victims often discourage individuals from pursuing legal action.<sup>35</sup>

Platform accountability presents another critical concern. Social media intermediaries play a central role in shaping online interactions, yet their responsibility in preventing and addressing harmful content remains limited. While the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021<sup>36</sup> impose certain due diligence obligations, enforcement is inconsistent, and compliance varies across platforms. Content moderation mechanisms are often opaque, slow, and inadequate in addressing the scale and speed of online abuse. Furthermore, algorithmic systems that prioritise engagement may inadvertently amplify harmful or abusive content, exacerbating the problem.

Underreporting is a significant barrier to effective enforcement. Many victims of online gender-based violence choose not to report incidents due to fear of stigma, social backlash, or lack of trust in the legal system. Cultural factors, including victim-blaming and societal pressure, further discourage reporting. In many cases, women are advised to withdraw from online platforms rather than seek legal remedies, thereby reinforcing the cycle of digital exclusion.<sup>37</sup>

Jurisdictional issues also complicate enforcement, as online offences often involve perpetrators and servers located in different regions or countries. This raises questions of legal authority, cooperation between agencies, and the applicability of domestic laws in cross-border contexts.

---

<sup>35</sup> Justice Verma Committee, Report on Amendments to Criminal Law (2013)

<sup>36</sup> Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021.

<sup>37</sup> Karine Nahon, 'Networked Governance and Gender Violence' (2016) *Information Society Journal* 1

Collectively, these challenges highlight the limitations of the current enforcement framework. Addressing them requires not only legal reforms but also institutional strengthening, improved technological capacity, enhanced platform regulation, and a more victim-centric approach to justice.<sup>38</sup>

## **6. Comparative Analysis: Global Legal Approaches to Online Gender-Based Violence**

A comparative analysis of international legal frameworks reveals a more structured and evolving approach toward addressing online gender-based violence (OGBV), offering valuable lessons for India. Several jurisdictions have moved beyond fragmented legal provisions to adopt targeted legislation and policy mechanisms specifically designed to tackle digital harms, particularly those affecting women.<sup>39</sup>

In the United Kingdom, laws such as the Malicious Communications Act and the Communications Act have been actively used to prosecute online abuse, while recent developments like the Online Safety framework aim to impose stricter obligations on digital platforms to monitor and remove harmful content. Similarly, the European Union has adopted a comprehensive regulatory approach through instruments like the Digital Services Act, which enhances platform accountability, mandates transparency in content moderation, and requires swift removal of illegal content. These measures reflect a shift towards holding intermediaries more directly responsible for user-generated harm.<sup>40</sup>

In the United States, while the First Amendment provides strong protection for freedom of speech, certain forms of online abuse are addressed through state-level laws and federal provisions targeting cyberstalking, harassment, and exploitation. However, the broad immunity granted to platforms under Section 230 of the Communications Decency Act has been a subject of ongoing debate, particularly in cases involving harmful online content.<sup>41</sup>

---

<sup>38</sup> Amanda Lenhart and others, 'Online Harassment' (2016) Pew Research Center Report.

<sup>39</sup> Henry Jenkins, *Confronting the Challenges of Participatory Culture* (MIT Press 2009)

<sup>40</sup> Tarleton Gillespie, *Custodians of the Internet* (Yale University Press 2018)

<sup>41</sup> Jack Balkin, 'Free Speech in the Algorithmic Society' (2018) 51 UC Davis Law Review 1149.

Australia has taken a more proactive stance by establishing the eSafety Commissioner, a specialised regulatory authority empowered to handle online abuse complaints, especially those involving women and children. This institutional innovation allows for quicker redressal mechanisms and greater victim support.

These international approaches demonstrate a trend toward recognising OGBV as a distinct legal issue requiring tailored solutions. Key elements include clearer legal definitions, stronger platform accountability, specialised enforcement bodies, and victim-centric remedies.

In contrast, India's current framework remains largely reactive and fragmented, relying on general provisions under existing laws. While recent regulatory developments indicate progress, there is still a lack of comprehensive legislation specifically addressing online gender-based violence.

Therefore, drawing from global best practices, India can strengthen its legal response by adopting a more cohesive and forward-looking approach that integrates legal reform, institutional capacity-building, and enhanced regulation of digital platforms.<sup>42</sup>

## **7. Conclusion and Reform Proposals: Towards a Safer Digital Space for Women**

The rise of digital technologies has undeniably expanded opportunities for women in India, enabling greater participation in education, employment, and public discourse. However, this progress has been accompanied by a parallel increase in online gender-based violence, reflecting the persistence of patriarchal structures within digital spaces. The concept of digital patriarchy underscores the reality that technology, rather than being inherently neutral, often reproduces and amplifies existing social inequalities.

This paper has demonstrated that while India possesses a range of legal provisions under the Information Technology Act, 2000 and the Indian Penal Code, these laws are fragmented and not specifically tailored to address the complexities of online gender-based violence. The absence of

---

<sup>42</sup> Apar Gupta, 'Free Speech and the Internet in India' (2015) NUJS Law Review 1

a clear legal definition, combined with procedural inefficiencies and limited enforcement capacity, significantly weakens the effectiveness of existing remedies. Moreover, challenges such as underreporting, lack of victim support, and inadequate platform accountability further exacerbate the problem.

The comparative analysis highlights that several jurisdictions have adopted more comprehensive and proactive approaches, including platform-specific regulations, specialised enforcement bodies, and victim-centric mechanisms. These models provide valuable guidance for India in reforming its legal and institutional framework.

In light of these findings, this paper proposes several key reforms. First, there is a need for a dedicated legal framework that explicitly recognises and addresses online gender-based violence as a distinct category of harm. Second, platform accountability must be strengthened through clearer obligations regarding content moderation, transparency, and algorithmic responsibility. Third, capacity-building initiatives for law enforcement agencies are essential to enhance technical expertise and ensure gender-sensitive handling of cases. Additionally, awareness campaigns and support mechanisms should be developed to encourage reporting and assist victims throughout the legal process.

In conclusion, ensuring a safe and inclusive digital environment for women requires a holistic approach that combines legal reform, institutional strengthening, and societal change. Only through such integrated efforts can the promise of digital empowerment be fully realised without compromising the dignity, safety, and rights of women in India.