DIGITAL VIOLENCE AS A BARRIER TO WOMEN'S EMPOWERMENT: GOVERNANCE, DEVELOPMENT AND INCLUSION IN INDIA

Ms. Purnima Sharma

Abstract:

Digital technologies are now defining the ways of learning, working and engaging in the public life of women in India, but the same digital shift opens possibilities of new types of violence which are directed against the bodies, identities, and voices of women. Technology enabled gender based violence, such as online harassment, non-consensual image sharing, doxxing and stalking, recreates existing gender hierarchies and exacerbates structural inequalities in online and offline spaces. These harms are further exacerbated by digital exclusion, and internet shutdowns especially to women at the margins like those in conflict-affected areas or by marginalised communities (Chochoi, 2025). Although such programmes as Digital India, e governance platforms and digital literacy programmes aim to increase the level of inclusion and access, they fail to fully account for the risks and harms that women experience in digital space or chilling effect of violence on their involvement. The paper is based on doctrinal and analytical approach to research how digital violence limits empowerment of women, challenges the sufficiency of Indian legal and policy frameworks and assesses governance and development programs through the prism of gender. It claims that digital violence is not merely a matter of cybercrime but fundamental development and governance issue, and that non- negligible inclusion means coordinated legal change, gender responsive digital governance and rights based digital citizenship by women.

Keywords: Digital violence; women's empowerment; cyber law; governance; inclusion

1.1. Introduction and Background of the Study

1.1.1.Context of the women empowerment in India.

Even with constitutional guarantees of equality and non-discrimination, women in India still have to bargain with multiple layers of inequality in the economic, social and political sphere. Research on women in the digital age in India reveals that women continue to be influenced by education levels, caste, region and income in their access to opportunities, mobility and decision-making power in their households and community (Choudhary and Patidar, 2024). Empowerment thus does not work in vacuum, but it is tied to material resources and enabling institutions and safe space in which women can voice their opinions without the fear of retaliation. It is also acknowledged by the courts that violence against women, in its many manifestations, has a direct negative impact on dignity and equality, and one example of such a case is Vishaka v. Article 14 and Article 21 protections were associated with workplace harassment in the State of Rajasthan, (1997) 6 SCC 241. The entry of digital tools into this terrain is subject to these already existing inequalities and can either create new avenues of empowerment or reinforce the historical patterns of control, and cause damage.

The economic empowerment of women is also affected by the digital technologies, as they change the ways women get access to markets, financial services and information, but these advantages are unevenly

distributed. The literature on digital literacy and gender equality highlights that the government has been trying to bridge the digital divide and ensure women can use devices and platforms, although social norms and safety issues tend to limit their real utilization (Sowmya et al., 2025). To a lot of women, especially in rural or conservative settings, families do still watch phone activity, limit social media access or dishearten online communication with strangers due to the perceived safety risks which are both sometimes factual and sometimes paternalistic. Jurisprudence of right to privacy and autonomy, especially Justice K.S. Puttaswamy (Retd.). v. Union of India, (2017) 10 SCC 1, confirms the fact that women are entitled to independent rights over their communications and personal data, but in daily digital life, it does not always correlate with these values. Empowerment is therefore disputed and unstable practice in the digital world.

1.2. Digital spaces in governance and development.

India is moving towards governance that is more digital with regard to service delivery, welfare transfers and citizen engagement, and establishing new interfaces between women and State. According to the Digital India vision, online channels, common service centres and mobile applications can deliver services on-demand, any-where, and will theoretically ease the load of travel and transaction costs, which is important to women with unpaid care obligations (Gurumurthy and Chami, 2018). The literature on e governance mentions though that this change also comes with its own set of challenges such as the lack of digital literacy, language difficulties and the absence of gender sensitive design in most public portals (Kaur & Singh, 2016). To overcome these platforms, women can use intermediaries, including local agents or male relatives, and in the process weaken privacy and control over personal information. Simultaneously, redress avenues at the same time are still disjointed and slow in the event of online harassment or fraud on or near government linked sites.

Reliance on digital identity systems and platforms have now filtered down to welfare, health and education schemes and this has a direct effect on the inclusion of women. Digital exclusion reporting of Manipur conflict demonstrates the role of connectivity blackouts and service outages in disconnecting women to information, emergency aid and basic governance procedures, trapping them in insecurity and marginalization (Chochoi, 2025). According to the feminist studies of digital governance, datafication and platformisation can reinforce new patterns of surveillance and control, especially in the cases when women do not have bargaining power to refuse to be collected or to object to the practices of profiling (Gurumurthy and Chami, 2018; UN Women, 2022). Laws that regulate these systems like data protection law and platform regulation, then, are highly instrumental in arbitrating the presence of empowerment or structural violence within the digital space.

1.3. Digital violence against women conceptualisation

The digital violence against women encompasses a broad range of actions, including abusive messages and non-consensual sharing of intimate pictures, identity theft, deepfake pornography and organized trolling. Online violence is described as a global issue by UN Broadband Commission as a wakeup call to the world since cyber violence, more frequently than not, is a reflection and continuation of offline gender-based violence and not a distinct phenomenon (UN Broadband Commission, 2015). The case study of gender-based violence in India technology also points out the fact that even the professionals in the country refer to the same issue as online gender based violence, cyber violence and online harassment, but they all concur that power dynamics and patriarchal culture are still the key forces in the digital arena (USAID, n.d.). This violence may occur on social media, chat apps, online games and other networked spaces, and may often include strangers, friends and intimate partners. These harms extend beyond the emotional distress to economic, social and political impacts such as loss of employment, education withdrawal and social isolation.

The difference between offline and online expressions of gender based violence is primarily in the instruments and speed of damage but not in the logic behind these manifestations. Technology enables the abuser to multiply the abuse quickly, store long-lasting replicas of the abusive material, and clear records or conceal under anonymity, making them difficult to police and prosecute. The Indian criminal and cyber laws (such as the provisions of Indian Penal Code on criminal intimidation, defamation and outraging modesty and the provisions of Information Technology Act on obscene material and child sexual abuse material) apply to most of the digital harms, but they do not fully cover the new practices such as deepfakes or non consensual image based extortion in clear and survivor centred way. International human rights norms such as Convention on Elimination of all forms of discrimination against women, as well as, General Recommendation No. 35 on gender based violence, require States to act on both offline and online aspects, but domestic practice tends to be slow. The clarity of concepts in relation to digital violence thus becomes important towards consistent law and policy.

1.4. Rationale on focusing on governance, development and inclusion.

Digital violence is not just abusive of individual rights, it also perverts the processes of governance and development. In cases where women experience long-term online harassment due to engaging in a debate in public space, criticising authorities or challenging elections, they will tend to self censor or leave online platforms, which compromises inclusive governance and democratic deliberation. Reports on women in Indian digital public life indicate that abuse may be directed at women leaders, journalists and activists with derogatory misogynistic and casteist remarks, threatening sexual violence or doxing personal information, which leads to climate of fear that transcends beyond individual actions (Choudhary and Patidar, 2024; USAID, n.d.). Even the well-constructed e governance platforms cannot achieve the participation objectives in such climate, as women are reluctant to participate in them to the full extent or to express their grievances. In this way, digital violence becomes an obstacle to substantive realisation of rights that are offered by formal laws.

Digital fear & exclusion also interplay with development programmes that depend on technology as one of the enablers. The success of any digital literacy programs will only be possible when women are convinced that the online environment is relatively secure and complaints will receive appropriate and appropriate timely attention. The guidance of UN Women on digital inclusion emphasizes that the gender analysis should focus on access, agency, norms and institutional accountability as a combined unit, instead of considering connectivity as neutral good (UN Women, 2022). The combined impact of violence, shutdowns and lack of tailored assistance, used in conflict or crisis situations, like Manipur conflict, endanger many women as offline and left behind during governance processes, thus posing a threat to the principle of leaving no one behind in sustainable development (Chochoi, 2025). Thus this paper identifies digital violence as a governance and development problem and not merely an issue of individual cybercrime and recommends combined solutions both at law, policy and institutional practice.

1.5. Research Problem

In India, digital violence against women is gaining traction on multiple platforms at a very broad spectrum, but the legal and institutional reaction remains disjointed and reactive. Cyber offence laws, general criminal law and women specific protections tend to work in isolation thus creating confusion to the survivors on the right forum to use, offences covered, and procedural protection. The technology based research in the field has captured gender based violence in India, that captures barriers to reporting, such as police reluctance, victim blaming attitudes and absence of specialised cyber forensic capabilities, which keep many cases unreported or downplayed (USAID, n.d.). Digital tools-based governance & development programmes often do not incorporate effective gender based risk analysis or survivor redress redirection into platform creation and action (UN Women, 2022). There is therefore scarcity of legal literature that

integrates digital violence with women empowerment, digital citizenship and inclusive governance in Indian context in a systematic manner that creates critical gap in analytical literature that is the aim of this paper to fill.

1.6. Scope and Limitations of the Study

The research aims at women and girls in India who access internet and other digital technologies such as mobile phone, social media, messaging applications and e governance sites. It focuses on gender based violence in the civilian setting that is aided by technology, including harassment, non consensual sharing of images and surveillance, and does not consider cyber warfare or national security operations. The legal analysis focuses primarily on laws, policies and some of the judicial cases of Supreme Court and major High Courts of the country, but recognizes that most of the implementation issues are played at state and local levels. Methodologically, paper is based on secondary literature, such as empirical studies and policy reports, as opposed to primary fieldwork, and thus does not provide any statistical measures of prevalence other than what is already reported in the literature (UN Broadband Commission, 2015; USAID, n.d.). These restrictions however permit specialized doctrinal and analytical treatment of fundamental problems.

1.7. Research Objectives

The paper pursues four closely related objectives that together frame enquiry into digital violence & women's empowerment. The research objectives are as follows:

1. To analyse how different forms of digital violence, including harassment, stalking & image based abuse, restrict women's economic, social & political empowerment in India.
2. To examine adequacy & coherence of Indian legal frameworks on cyber law, criminal law & women protection law in addressing technology facilitated gender based violence, with specific reference to Information Technology Act, Indian Penal Code & special legislation on violence against women.
3. To evaluate governance & development initiatives such as Digital India, e governance portals & digital literacy programmes through gender & inclusion lens, drawing on research that applies gender lens to digital policy.
4. To develop reform oriented recommendations for strengthening legal protections, institutional mechanisms & digital governance practices to build safer & more inclusive digital ecosystem for women.

1.8. Research Questions

The enquiry unfolds through four central research questions that guide doctrinal & analytical discussion. The research questions are as follows:

1. How digital violence operates as structural barrier to women's empowerment & digital citizenship in India, focusing on everyday experiences as well as high profile cases of online abuse documented in recent studies?
2. Whether existing Indian cyber, criminal & women protection laws provide sufficient, clear & survivor centred responses to technology facilitated gender based violence, or whether gaps & inconsistencies persist in definitions, procedures & enforcement?
3. How governance & development programmes that promote digital tools, including Digital India & various e service delivery schemes, may inadvertently reproduce digital gender gaps or fail to protect women from harm?
4. What legal, institutional & policy measures could better integrate gender responsive approaches to digital violence, ensuring meaningful participation & inclusion of women across diverse social locations?

1.9. Research Hypotheses

The study proceeds on basis of four working hypotheses that draw from existing literature & legal developments. The research hypotheses formulated are as follows:

1. That digital violence significantly limits women's participation in online public life by inducing fear, self censorship & withdrawal from digital spaces, thereby weakening democratic engagement & accountability.
2. That Indian legal frameworks on digital violence remain fragmented & under enforced, with important provisions either outdated or applied unevenly, which leaves survivors without timely & effective remedies, despite constitutional guarantees of equality & dignity.
3. That governance & development initiatives related to digital technologies insufficiently integrate gendered digital lens, thus failing to anticipate or mitigate risks for women, as indicated by analyses of Digital India & e governance initiatives.
4. That stronger legal protections, coupled with inclusive & participatory digital governance practices, can substantially enhance women's empowerment & digital inclusion when implemented with accountability & adequate resources.

1.10. Research Methodology

The paper is based on the methodology of doctrinal research, which is based on the close reading of the statutory provisions, policy documents and judicial decisions on digital violence, women rights and cyber law in India. It examines important provisions of Information Technology Act, Indian Penal Code and special laws on violence against women, as well as constitutional provisions on equality, freedom of expression and privacy in order to comprehend the normative framework of digital harms. Analytical review of secondary literature, such as international and national reports on cyber violence against women, digital gender divides and digital inclusion, is also used to provide a context of legal rules in the broader social realities (UN Broadband Commission, 2015; USAID, n.d.; Gurumurthy and Chami, 2018; UN Women, 2022; Sowmya et al., 2025). Evaluation of State obligations and policy decisions is informed by comparative perspectives and international human rights standards, including CEDAW and Beijing Platform for Action, but is primarily focused on Indian context. All along, methodology is interpretive and normative, aiming at identifying gaps, tensions and possibilities of prevailing legal order, as opposed to creating new empirical data.

1.11. Conceptual Framework – Digital Violence and Women's Empowerment

Conceptualizing digital violence against women in India

The continuum of behaviours that constitute digital violence against women in India includes behaviours that seek to silence, humiliate, control or exploit women in networked spaces. Such behaviours comprise abusive messages, doxxing, morphing pictures, non consensual posting of intimate material, deepfakes, impersonation and continuous surveillance with spyware or stalkerware, all of which are based on digital technologies but represent long-standing patriarchal practices (UN Broadband Commission, 2015; USAID, n.d.). Research shows that women who talk about politics, gender justice or minority rights are more often subject to online abuse, and in addition to their opinions, their bodies, families and perceived morality are also attacked (Choudhary and Patidar, 2024). The legislation struggles to classify such harms, occasionally falling under such offenses as criminal intimidation or obscenity, occasionally using information technology legislation, which does not necessarily address gendered aspect of violence. Such a discrepancy between the experience of living and the legal status leads to under reporting and frustration among survivors.

Patterns and visibility of digital violence are shaped by platforms and technologies, since each space is conducive to various forms of anonymity, amplification and moderation. Different types of abuse exist on social media sites, end to end encrypted messages services and short video apps, though cross platform spill over is frequent as the content spreads quickly and search engines index dangerous content. The Manipur conflict report shows how the connectivity and social media can simultaneously reveal and amplify ethnic and gendered violence, and that shutdowns subsequently eliminate avenues to support and accountability (Chochoi, 2025). The global human rights institutions are progressively identifying that under CEDAW, States have a duty to make sure that non-state actors, such as platforms, take due diligence to avert, investigate and rectify gender based online violence. In India, the discussion of intermediary liability and safe harbour of platforms in Information Technology Act consequently has a direct application to the practice of preventing and addressing digital violence.

1.12. Women empowerment and citizenship in the digital era

Empowerment of women in the digital age should involve the capacity to utilize technology to find information, give opinions, establish networks and demand entitlements without undue risk of being harmed. The research on digital literacy emphasizes that skills are not a sufficient condition to be empowered, women must have supportive social settings, have control over gadgets and trust in institutions that manage their data and complaints (Sowmya et al., 2025). In cases where women are afraid that any online presence can result in harassment or abuse of images, they can restrict their use to a strictly instrumental or family-supervised one, which lessens the transformative possibilities of digital tools. Constitutional law which supports individual freedom, privacy and expression, like Shreya Singhal v. Union of India, (2015) 5 SCC 1, confirms the significance of free speech on the internet but also poses a challenge of how to deal with the harmful speech that is directed at the dignity and safety of women. These interests demand delicate legal and policy solutions that preempt the agency of women.

There is also a relationship between digital citizenship and political empowerment, as online spaces are becoming a more common area of debate, campaigning and mobilisation on matters of public concern. When women challenge elections, head movements or criticize policies on online platforms, organized digital violence can intimidate not just them but other women who watch backlash on going out. The e governance and digital participation gender analysis reveals that these power dynamics need to be tackled through inclusive design by offering safe feedback, complaint and collective organising channels (Gurumurthy and Chami, 2018; Kaur and Singh, 2016; UN Women, 2022). The international frameworks such as Beijing Platform for Action have prioritized women to have equal participation in media and new communication technologies as a key to gender equality, and this means that the States must consider digital citizenship to be a substantive right and not a privilege. Thus, the conceptual framework on the empowerment should consider digital violence as direct assault on citizenship and not an issue of personal safety.

1.13. Violence, Empowerment and Inclusion Analytical Framework

A critical framework of this paper is connected with digital violence, empowerment and inclusion using the notions of fear, surveillance and intersectionality. Fear is a mechanism that limits behaviour; when women expect to be abused or to damage their reputation, they pre- emptively leave some platforms or subjects, which limits personal and collective empowerment. Digital tools can be used to survey and manipulate the movements and communications of women by intimate partners, families, communities or State, as reported in the global and Indian reports of technology used to control women (UN Broadband Commission, 2015; USAID, n.d.; Chochoi, 2025). Intersectionality makes us remember that women are not equally vulnerable to digital violence; caste, religion, sexuality, disability, region and exposure to conflict influence vulnerabilities and resources to resistance. In this way, Dalit women activists, queer

users or women in conflict zones tend to experience more severe and less socially recognised types of digital violence, but mainstream policy might ignore them.

It is also in this framework that inclusion policies that are so limited in their attention to connectivity, the distribution of devices or skills training can lead to a further entrenchment of inequalities once power relations and safety are overlooked. The guidance on digital inclusion by UN Women claims that gender analysis should not be limited to access but agency, norms and institutions, inquiring who controls technology and who gains by data driven systems (UN Women, 2022). The application of this lens to the Indian legal and policy frameworks would mean evaluating the extent to which the cybercrime cells, data protection agencies and e governance agencies are using gender expertise, disaggregated data and survivor centred processes in their day-to-day work. The global tools like CEDAW and General Recommendation No. 35 challenge the States to implement multi-faceted strategies that incorporate law reform, prevention, protection and redress to gender based violence even in the digital environment. The analytical construct in this paper thus places the digital violence in the context of larger struggle of substantive equality, democratic governance and development justice to women in India.

1.15. Legal And Policy Framework of Digital Violence in India.

1.15.1. Analysis of applicable criminal and cyber legislation

The patchwork framework of Indian criminal law and cyber law combined can help deal with most types of digital violence against women. Sexual harassment, stalking, voyeurism, criminal intimidation, defamation and insulting modesty of women are criminalized in the Indian Penal Code, 1860, and currently in Bharatiya Nyaya Sanhita, 2023, which are also increasingly taking digital forms like abusive messages or non consensual sharing of images. Criminal intimidation / insult provisions work when the threats or obscene statements are made against women via the phone, email or social media, but the police often consider such actions to be minor. This is supplemented by the Information Technology Act, 2000 which penalises publication or transmission of obscene or sexually explicit material, child sexual abuse material and breach of privacy as a result of unauthorised image capture or sharing. The identity theft, cheating by personation and unauthorised access sections take on a new dimension when the abusers break into accounts, impersonate women or open up fake profiles to harass or defraud them via the Internet.

These provisions interrelate with special legislation that safeguards children and regulates sexualised representation which is frequently confluent in the online world. Protection of Children from Sexual Offences Act, 2012 criminalises the use of children in pornography, grooming and online sexual exploitation and is applicable in cases where the perpetrators distribute images or videos of minors via messaging applications or web sites. The Indecent Representation of Women (Prohibition) Act, 1986 discusses objectifying images of women, and it is now being discussed in policy circles as to whether its application to online advertising, streaming media and social media campaigns should be strengthened. Shreya Singhal v. the Supreme Court. Union of India, (2015) 5 SCC 1 overturned section 66A of Information Technology Act as being vague and having a chilling effect on free speech, but made it clear that other obscenity, defamation and incitement laws were still enforced on-line. This ruling indirectly influences the manner in which cases of digital violence are being framed, and it demonstrates that constitutional scrutiny is at the heart of the process of creating new cyber offences.

1.15.2. Women protection frameworks and data related frameworks

The implications of women specific laws and institutional mechanisms to digital harms, are also that they address gender based violence as structural issue, as opposed to an isolated misconduct. Physical, sexual, verbal, emotional and Economic abuse of women, including technology mediated surveillance, humiliation

or economic control, such as seizure of devices or surveillance of messages, are also addressed by Protection of Women from Domestic Violence Act, 2005. The Sexual harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013, is based on Vishaka v. The case of State of Rajasthan, (1997) 6 SCC 241 is applicable when sexually coloured messages are sent by colleagues, offensive memes are shared or hostile group chats are created. Changes in criminal law following Delhi gang rape case added offences of stalking and voyeurism, which now reflect in tenacious online following, non consensual recording and sharing of private acts. These models bring about continuum in principle between offline and online violence, but victims continue to find it difficult to persuade institutions that digital abuse is real harm.

The new law of data protection and privacy is another important layer since most of the digital harms are associated with the abuse of personal data or intimate content. The Supreme Court in the case of Justice K.S. Puttaswamy (Retd.). v. Union of India, (2017) 10 SCC 1 acknowledged privacy as a fundamental right and emphasized informational self determination and this reinforces the objection to non consensual sharing of images, doxing or spying. When the Digital Personal Data Protection Act, 2023, comes into effect, processing of personal data by State and privates will be regulated, as well as principles like consent, purposes restriction and security protection may be used to claim in cases where a platform or intermediary does not protect the data of women. Feminist critique of digital governance in India cautions though that data regimes should incorporate gender and power relations, otherwise, they can reinforce surveillance and control instead of empowerment (Gurumurthy and Chami, 2018). The advice of UN Women on digital inclusion also highlights that privacy & security are essential to meaningful digital inclusion, particularly when it comes to women experiencing intersecting discrimination (UN Women, 2022).

1.15.3. Policy programs on safety and enforcement issues online

Government policy efforts focus on online safety and digital literacy of women, but are still disjointed and even gender-thin. National cybercrime reporting portals, police cyber cells and awareness campaigns are encouraging citizens to report online abuse, phishing and financial fraud, and a range of programmes under Digital India are supporting basic digital skills to women and girls, particularly in rural locations (Sowmya et al., 2025). A study on the digital literacy and gender equality in India observes that such efforts can empower women into socio economic inclusion, however, it also points out the disparities in long term funding, support in local languages and customized content on gender based online violence (Sowmya et al., 2025). The gender based violence case study documents published by the USAID technology enable gender based violence case study facilitation in India that states that most civil society organisations currently operate helplines and legal support services, but even then survivors do not know which portal, police unit or tribunal has jurisdiction over their complaint (USAID, n.d.). This misunderstanding usually results in unnecessary referrals and delays.

Critical evaluations on enforcement indicate that there have been cases of under reporting, insensitive policing methods and low conviction rates on cases of technology facilitated violence. According to the experts interviewed in India case study, victim blaming, inadequate knowledge of platform architecture and absence of cyber forensic skills are the primary challenges in the law enforcement agencies (USAID, n.d.). The jurisdictional problems are in cases where the perpetrator and servers are in different states or countries, and local police are forced to rely on slow mutual assistance procedures or unresponsive platforms. The Information Technology Act and its 2021 rules on intermediate liability have mandated that unlawful content should be promptly removed on notice, but women are frequently subject to delays, inconsistent standards and nontransparent decision-making. The report by the UN Broadband Commission on cyber violence points at the same issues across the world, with the commission warning that the laxity in enforcement and the lack of transparency among intermediaries can become the new normal and encourage women to distrust formal systems further (UN Broadband Commission, 2015). Incorporating online harms

into larger violence against women systems thus is still a pressing, incomplete job.

1.16. Governance, Development and Digital Inclusion – A Gendered Assessment

1.16.1. Digital India and e governance Gender lens

E governance reforms & Digital India programme will bring quicker and more open service delivery, but the effect on women will be determined by access, safety and agency. The gender based study reveals that women still have unequal access to devices, connectivity and digital services, and the rural women, poor women and women in marginalised communities are subjected to compounded disadvantages of cost, mobility and literacy (Choudhary and Patidar, 2024). The Digital India through gender lens study holds that digital public infrastructure may or may not democratise access, but will increase exclusion, based on how platforms manage identity verification, language options and grievance redress (Gurumurthy and Chami, 2018). Harsimrat Kaur and Hamraj Singh point out that the policy of e governance in India seldom incorporates the perspectives of women, which results in the design decisions that presuppose a generic, male user and neglects the limitations that women may face, such as the fear of going to cyber kiosks or giving out their credentials to intermediaries (Kaur and Singh, 2016). When these larger obstacles are combined with digital violence, lots of women prefer limited or moderated consumption of e services.

There are other types of digital exclusion to conflict-affected and remote areas which have a direct impact on the way women participate in governance. The Manipur conflict study demonstrates how long term internet shutdowns, broken infrastructure and surveillance fears disturbed access to information, welfare schemes and complaint mechanisms to women leaving them offline and left behind in the governance processes (Chochoi, 2025). The women in these areas do not have easy access to online grievance portals over domestic violence, cyber harassment or welfare denial, but have to depend on informal networks which might not be legally binding. The digital inclusion guidance by UN Women emphasizes the idea that gender analysis in this situation should not solely focus on connection availability but also on safety, affordability and socio political risks (UN Women, 2022). The absence of such analysis means that the digital governance reforms will only contribute to the existing inequalities, as the benefits will go to those who are already connected, and women in unstable environments will face the dual burden of physical insecurity and digital invisibility.

1.16.3. Technology supported the shortage of violence and participation

Gender based violence through technology also creates severe lack of participation in digital democratic and civic space. The case study on technology in India enabled gender based violence reports to indicate that women politicians, journalists, activists and students who speak on controversial matters are subjected to aggressive campaigns of abuse, including rape threats, caste slurs, doxxing and spreading of doctored images (USAID, n.d.). According to the UN Broadband Commission, cyber violence causes chilling effect in the sense that most women self censor, abandon sites or avoid leadership positions to avoid attacks (UN Broadband Commission, 2015). Choudhary and Patidar explain that in India, women in the digital era tend to navigate the social media cautiously, creating a limited profile or quitting after negative experiences, which negates the potential of the social media in terms of political education and mobilisation (Choudhary and Patidar, 2024). Such trends are not personal vulnerabilities but institutional aggression in online social spaces.

Acknowledgment of rights to equality, dignity, speech and participation in the law is not necessarily reflected in safe Internet environments. Cases such as Shreya Singhal v. courts. Union of India, (2015) 5 SCC 1 have been right to insist on the protection of legitimate political speech against overcriminalisation, but same jurisprudence leaves unanswered complex questions of regulating targeted, gendered abuse without chilling dissent. Feminist scholars consequently state that States should implement comprehensive

approaches that integrate narrow criminal provisions with positive duties to defend the involvement of women, including rapid response teams, platform regulation and support to counter speech movements (Gurumurthy & Chami, 2018; UN Women, 2022). In places where such measures are still ineffective, the online abuse is an effective way to limit the digital citizenship and leadership of women, despite their hypothetical access to devices and connections. This lack of connection between formal rights and substantive participation is at the core of the digital inclusion debates.

1.16.4. Digital exclusion, governance failure and structural barriers

India case based insights emphasize the role of digital exclusion and governance failures in enhancing each other and increasing gendered harms. The Manipur conflict paper records how the women could not access helplines, government advisories and legal information due to shutdowns, as well as conceal evidence of violence distributed via digital platforms (Chochoi, 2025). Women reported fear of surveillance and reprisals in case they used virtual private networks or other communication tools which further limited reporting of abuses. Similarly, Gurumurthy and Chami note that the centralised design of platforms and the opaque governance of the algorithms in the public systems may exclude the voice of the local, particularly that of women, who are not digitally fluent or lack supportive intermediaries (Gurumurthy and Chami, 2018). In her study of the e governance policies, Harsimrat Kaur mentions that the lack of gender disaggregated data complicates the analysis of whether the digital services are delivered to women or lower their transaction costs (Kaur and Singh, 2016). In the absence of such information, accountability systems are feeble.

There are also structural and institutional barriers due to poor coordination between institutions of justice, telecom and social welfare. The digital inclusion advice of UN Women emphasizes that meaningful inclusion involves cross sectoral collaboration, since connectivity, content, capacity and safeguards interact in complex ways (UN Women, 2022). Practically, police cyber cells, women commissions, telecom regulators and social welfare departments are usually operating in silos and there is not much sharing of information or even a common protocol to follow when receiving reports of digital violence. According to the USAID India case study, survivors occasionally transfer between the police stations, women helplines and platform complaint systems without clear instructions or prompt relief (USAID, n.d.). Such fragmentation burns out survivors and is an indication that institutions are not taking technology facilitated abuse as a serious governance concern. These structural obstacles need to be tackled with not only new legislation but also with institutional cultures that appreciate gender justice and digital rights.

1.17. Towards A Safer and Inclusive Digital Ecosystem for Women

Enhancement of the law on digital violence

Enforcement of legal framework on digital violence in India needs better definitions, harmonisation of provisions and survivor centred procedures. International reports suggest that States should specifically understand technology enabled gender based violence in legislation, including non consensual intimate image sharing, doxxing, cyberstalking and deepfake pornography, without undermining protections against legitimate speech (UN Broadband Commission, 2015; USAID, n.d.). The lawmakers in India can take a chance to unify fragmented offences in Information Technology Act, penal code and special laws into consistent chapter on digital violence against women and children, elucidating the aspects, defences and redress. This would assist police and prosecutors to frame cases appropriately and reassure victims that law is talking directly to them. Harmonisation must also provide similar conduct with similar liability, whether it is done online or offline.

Reforms should also be careful not to go too far in drafting reforms that criminalize dissent or minority

opinion in the name of protecting women. Jurisprudence Singhal, v. Shreya Singhal.

Union of India, (2015) 5 SCC 1 and Justice K.S. Puttaswamy (Retd.). v. Union of India, (2017) 10 SCC 1 demonstrates that any additional limitations on digital expression or data processing will be subject to constitutional review on the grounds of vagueness, proportionality and necessity. This constitutional prism must be used in drafting, whereby specific language is encouraged, specific mens rea requirements and robust procedural protections are promoted. According to international human rights frameworks, such as CEDAW General Recommendation No. 35, States should implement far-reaching measures that cut across criminal, civil and administrative law, such as compensation, protection orders and duties of due diligence of platforms. The inclusion of these standards in Indian reforms can help in the balanced and rights respectful approach to digital violence.

Institutional & procedural reforms

Institutional and procedural reforms are equally significant since even powerful laws cannot work where institutions are powerless or insensitive. The case study on the USAID India reveals that specialised gender expert cyber units are required to support the upgraded forensic infrastructure and standard operating procedures to deal with technology facilitated abuse (USAID, n.d.). The police, prosecutors and judicial officers need to be trained regularly on platform architectures, preserving evidence, mutual legal assistance and trauma informed interviewing with survivors. Liaison with the women cells and one stop centres can be used to make sure that the survivors get psychosocial assistance as well as legal assistance. Practices in the context of digital exclusion, including Manipur, also reflect the necessity of contingency plans to support the reporting channels and protection systems in the case of network outages (Chochoi, 2025). Such plans might incorporate the offline complaint systems that will eventually be incorporated into the digital case management systems.

The procedural innovations may also decrease the burdens on survivors and increase accountability. Re victimisation can be avoided by fast track procedures of content takedown orders, in camera hearings of sensitive digital evidence and simplified procedures of cross jurisdictional complaints. According to the work on digital governance by Gurumurthy and Chami, the institutional reforms would also incorporate the public oversight institutions that can audit the enforcement practices, monitor compliance with the platforms and accept complaints regarding system failures (Gurumurthy and Chami, 2018). These bodies may consist of the representatives of women organisations, technical experts and privacy advocates, which would guarantee a variety of points of view. The absence of these institutional upgrades will mean that the survivors will still face hostile environments, and digital violence will still be forced in the category of harm even with the formal legal status.

Digital gender responsive policies of governance and development

Gender responsive digital governance demands that all significant digital programmes and platforms should incorporate gender analysis during its lifecycle. The recommendations of UN Women regarding digital inclusion suggest that policymakers should analyze access, agency, norms and institutional accountability prior to the introduction of new technologies, and this strategy can be implemented in the Indian context where social hierarchies are highly influential in determining digital use (UN Women, 2022). The e governance portals and digital identity systems in Digital India projects must then perform ex ante gender impact assessment, consult women groups when designing and develop special indicators to monitor women usage, satisfaction and safety. According to Gurumurthy and Chami, digital public infrastructure should incorporate the principles of equity and data justice, such as the minimum amount of data collected, the high level of protection and the opportunity to have a recourse in case of a system failure (Gurumurthy and Chami, 2018). These values explicitly safeguard the women who can be more vulnerable to data breaches or profiling.

The policy frameworks must also have in place grievance mechanisms on the public platforms, which are accessible, technology responsive, and survivor friendly. The inclusion of e governance analyzed by Harsimrat Kaur refers to the significance of local intermediaries that can help women to file complaints and navigate the portals, assuming that they adhere to the rules of confidentiality and consent (Kaur and Singh, 2016). The authorities need to think in terms of connectivity contingency, multilingual communication and safeguard human rights defenders of women who record abuses in digital formats in conflict or unstable environments (Chochoi, 2025). By incorporating gender disaggregated data into the monitoring system, it may be possible to determine areas or communities where women are digitally marginalized or disproportionately victims of online abuse. This can be then fed back to policy and resource allocation corrections in the course of the course.

Community, education, responsibility of the private sector and way forward

The combination of community based education and responsibility of the private sector constitute the daily circumstances of the digital lives of women. The studies about digital literacy and gender equality in India demonstrate that the government programs can increase skills and confidence, yet the community norms and family values have a powerful impact on whether women apply their knowledge to empowerment or stay limited (Sowmya et al., 2025). Male engagement and involvement in programmes that address male norms of respect, consent and bystander intervention can change cultures that currently legitimize online abuse. The UN Broadband Commission emphasizes that prevention programs must be based on both raising awareness and providing tangible support networks, like hotlines, legal aid and counselling, so that victims can have a practical choice, not just a slogan (UN Broadband Commission, 2015).

There are also serious responsibilities of due diligence and content governance of private platforms. According to the case study of the USAID India, the experts of the civil society demand faster response rate, better community norms, significant appeal procedures and periodic disaggregated transparency reports by gender and geography (USAID, n.d.). The joint effort by regulators, platforms and women organisations can devise standard procedures in responding to technology enabled gender based violence, such as proactive identification of non consensual intimate images and doxxing. The contexts of digital exclusion experienced remind policymakers that connectivity policies, decisions of shutdown and surveillance practices should also undergo gender equality tests, as women are the ones who pay disproportionate costs when governance crises are played out online and offline (Chochoi, 2025). To continue, safer and more inclusive digital ecosystem of women in India will require long-term partnership between institutions, law makers, communities and private actors based on feminist understanding of power, rights and justice in digital age.

1.18. References

1. Choudhary, A., & Patidar, R. (2024). Women in digital age in India. *The World Research of Political Science Journal, 7*(1), Article 1.
2. Chochoi, J. (2025). *Offline & left behind: Digital exclusion, gender & governance crisis in Manipur conflict*. IT for Change.
3. Gurumurthy, A., & Chami, N. (2018). *Digital India through gender lens*. IT for Change.
4. *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1 (India).
5. Kaur, H., & Singh, H. (2016). E governance & its challenges: Inclusion of women in e governance policy in India. *AIMA Journal of Management & Research, 10*(2/4).
6. *Shreya Singhal v. Union of India*, (2015) 5 SCC 1 (India).
7. Sowmya, B. N., Deepthi, K. H., & Nandapriya, B. N. (2025). Digital literacy & gender equality: A mechanism for facilitating women's empowerment in twenty first century. *International Journal of*

Creative Research Thoughts, *13*(8), IJCRT2508605.

8. UN Broadband Commission. (2015). *Cyber violence against women & girls: A world wide wake up call*. Working Group on Broadband & Gender.

9. UN Women. (2022). *Gender analysis in technical areas: Digital inclusion – Guidance note*. UN Women.

10. United States Agency for International Development. (n.d.). *Technology facilitated gender based violence in Asia: India case study*. USAID, NORC at University of Chicago, & International Center for Research on Women.

11. *Vishaka v. State of Rajasthan*, (1997) 6 SCC 241 (India).