World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Digital Gender Violence in Sri Lanka: A review of emerging trends, legal frameworks and policy gaps

Dinesh Deckker [1,*] and Subhashini Sumanasekara [2]

[1] *Department of Science and Technology, Wrexham University, United Kingdom.*
[2] *Department of Computing and Social Sciences, University of Gloucestershire, United Kingdom.*

World Journal of Advanced Research and Reviews, 2025, 27(03), 1933-1946

Publication history: Received on 20 August 2025; revised on 25 September 2025; accepted on 29 September 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.27.3.3367

Abstract

Digital Gender Violence (DGV) is a rising concern in Sri Lanka, manifesting through cyberstalking, image-based abuse, doxing, and impersonation. These harms disproportionately affect women, LGBTQ+ persons, and other marginalised groups. Despite growing public awareness, legal and policy responses remain fragmented and underdeveloped. This review addresses a critical gap by synthesising emerging trends, legal frameworks, and international best practices through an interdisciplinary, gender-sensitive lens. The study aims to answer four key questions: the nature of DGV manifestations, the effectiveness of existing legal and regulatory frameworks, the gaps in policy, enforcement, and digital literacy, and how international models can inform Sri Lankan reform.

A narrative review method was employed, integrating peer-reviewed literature, legal documents, and institutional reports from 2015 to 2025. Thematic analysis was guided by feminist theory and digital governance perspectives.

Findings reveal that legal instruments, such as the Online Safety Act (2024), lack precise definitions and clarity in enforcement. Policy coordination is weak, digital literacy remains low, and platform accountability is minimal. Vulnerable populations face compounded risks due to intersectional barriers related to gender, class, disability, and sexuality. Comparisons with Australia, Canada, and the Philippines highlight legal innovations that could be adapted to the Sri Lankan context.

This review contributes a structured, critical analysis of DGV in Sri Lanka, advocating for survivor-centred legal reform, inclusive education, and mandatory platform regulation. The study underscores the urgency of a comprehensive, rights-based national policy on digital gender violence and suggests future research should prioritise underrepresented groups and longitudinal data.

Keywords: Digital Gender Violence; Sri Lanka; Online Harassment; Feminist Legal Theory; Intersectionality; Online Safety Act; Gender-Based Violence

1. Introduction

Digital platforms have transformed social interaction. However, they have facilitated new forms of gendered harm. In Sri Lanka, women and gender-diverse individuals face harassment, image-based abuse and threats online. Such phenomena fall under the broader category of digital gender violence (Butler, 1990; Gill, 2017).

Research on digital gender violence in Sri Lanka is emerging but still fragmented. A thematic qualitative study found that Sri Lankan university students experience non-consensual image sharing, impersonation, and online defamation

* Corresponding author: Dinesh Deckker

(Harasgama and Jayamaha, 2023). Online gender-based violence manifests across age groups and sexual identities, causing serious harm to mental and social well-being (Search for Common Ground, 2024).

The Sri Lanka Computer Emergency Readiness Team (SLCERT) reported 3,566 cybercrime incidents in 2019, prior to the COVID-19 pandemic. During the pandemic, incidents drastically increased, with 16,376 reported in 2020 and 18,214 in 2021. In 2021, a significant majority of these incidents, 16,975, were related to social media, indicating a rising trend of online harm (Search for Common Ground, 2024).

The prevalence of online harassment against women is high. A recent study found that 85% of women parliamentarians in the Asia-Pacific region experienced online attacks from the public, indicating a significant aspect of online violence within this specific demographic (Inter-Parliamentary Union, 2025). Sri Lankan victims report patterns consistent with global trends, such as trolling, doxing, and cyberstalking (Search for Common Ground, 2024). Sri Lanka also faces legal and policy shortcomings in addressing these new forms of harm (Perera, 2011; Rajapaksha, 2023).

Foundational theories underpin this review. Butler's concept of normative violence (1990) helps explain how gendered harassment polices online identity. Gill's (2017) work on digital objectification sheds light on how women's bodies become targets. Haraway's (1991) cyborg metaphor situates online abuse in techno-social assemblages. Combined with sociolinguistic insights from Labov (1972), they provide a robust framework for analysing online discourse and gender-based harm.

However, regional research on digital gender violence often lacks the integration of theory, empirical evidence, and comprehensive legal analysis. Global reviews of technology-facilitated gender-based violence (TFGBV) consistently critique fragmented legal responses and weak enforcement, a challenge particularly pronounced in low- and middle-income countries (LMICs) (OECD, 2025; United Nations Population Fund, n.d.). The situation in South Asia mirrors this gap, as evidenced by challenges in Sri Lanka's policy and legal framework for addressing cyber sexual and gender-based violence (Search for Common Ground, 2024).

In Sri Lanka, the recently enacted Online Safety Act (2024) established an Online Safety Commission with the power to criminalise "prohibited statements" online (Amnesty International, 2024; Global Network Initiative, 2024). This legislation has drawn significant criticism from civil society, which argues that it risks overreach and may suppress free speech due to its vague definitions and broad discretionary powers (Amnesty International, 2024; Global Network Initiative, 2024). As of yet, no peer-reviewed study has assessed the specific implications of this Act for victims of digital gender violence.

To date, no comprehensive review addresses digital gender violence in Sri Lanka by combining theoretical, empirical and legal perspectives. The existing literature is disjointed, primarily qualitative, and often focuses on university populations. There is a need to synthesise international best practice, local evidence and legal frameworks to guide policy and research.

This review examines digital gender violence in Sri Lanka through three analytical lenses:

- Emerging trends and forms of violence, including harassment, doxing, cyberstalking and image-based abuse.
- Legal frameworks and enforcement, with a focus on the Online Safety Act and existing cybercrime and GBV laws.
- Policy and programme responses, including digital literacy, platform regulation and reporting systems.

1.1. Research questions

Four key questions guide this study

- What are the main manifestations of digital gender violence in Sri Lanka?
- How effective are existing legal and regulatory frameworks?
- What gaps remain in policy, enforcement, and digital literacy?
- Which international best practices can inform Sri Lankan responses?

1.2. Significance of the review

This paper makes several significant contributions:

- It provides a structured synthesis of digital gender-based violence in Sri Lanka.
- It analyses the adequacy of recent legal reforms and identifies enforcement challenges.
- It highlights deficiencies in policy and digital literacy interventions.
- It synthesises global best practices to inform future Sri Lankan action.

2. Methodology

This study adopts a narrative review approach to synthesise interdisciplinary knowledge on digital gender violence (DGV) in Sri Lanka. The review integrates legal analysis, gender theory, and empirical findings across multiple disciplines. The methodology prioritises conceptual clarity, source credibility, and contextual relevance.

2.1. Research Design

A qualitative, desk-based research design was employed. The study systematically reviewed academic literature, legal documents, and institutional reports related to DGV, focusing on Sri Lanka while incorporating comparative insights from South Asia and the global context. The review is narrative rather than systematic, allowing interpretive depth and theoretical integration.

This method was chosen to explore complex, multifaceted issues surrounding DGV—legal ambiguity, policy fragmentation, intersectional vulnerability, and socio-cultural dynamics—that purely quantitative methods cannot adequately capture.

2.2. Inclusion Criteria

Sources were selected based on the following criteria:

- Peer-reviewed journal articles published between 2015 and 2025
- Academic books from recognised publishers (e.g., Routledge, Harvard University Press)
- Institutional reports from UN Women, ITU, UNESCO**,** and regional organisations
- Legal documents and Acts (e.g., Sri Lanka's Online Safety Act, Penal Code, Computer Crimes Act)
- Relevant Sri Lankan or South Asian research, with emphasis on gender, law, or media studies

Only English-language sources were included. Preference was given to works that addressed gender-based violence, online harm, legal reform, digital governance, or intersectionality.

2.3. Exclusion Criteria

The following sources were excluded:

- Blog posts, newspaper articles, or unverified online commentary
- Grey literature lacking institutional authorship or peer review
- Outdated works not engaging with digital technologies or post-2015 policy changes
- General cybercrime literature does not address gender-based harms

This exclusion ensured analytical rigour and academic reliability.

2.4. Data Collection Process

Relevant sources were identified through targeted database searches, including:

- Scopus**,** Web of Science**,** and JSTOR for peer-reviewed academic articles
- Google Scholar **and** EBSCOhost for books and reports
- Official government websites (e.g., Parliament of Sri Lanka**,** Ministry of Women and Child Affairs) for legal documents
- Institutional repositories (e.g., UN Women**,** ITU**,** Commonwealth Secretariat) for policy reviews

2.5. Data Analysis Strategy

Thematic synthesis was used to organise the data into key domains:

- Manifestations of DGV
- Legal and institutional frameworks
- Policy and educational gaps
- Intersectionality and vulnerable groups
- International comparisons and best practices

These themes aligned with the research questions and the review's structure. Sources were interpreted through a gender studies lens, incorporating the work of foundational theorists such as Judith Butler**,** Rosalind Gill**,** and Donna Haraway**,** alongside legal analysis from feminist jurisprudence and digital governance scholarship.

A cross-comparative lens was applied in evaluating international legal models, identifying parallels and divergences relevant to the Sri Lankan context.

2.6. Ethical Considerations

As this review did not involve human subjects or primary data collection, formal ethical clearance was not required. However, all sources were cited appropriately following APA 7 referencing standards. Care was taken to represent vulnerable groups with sensitivity and to avoid reinforcing harmful stereotypes.

3. Literature review

3.1. Defining Digital Gender Violence: Conceptual and Theoretical Foundations

Digital gender violence (DGV) refers to harmful, hostile, or abusive behaviour targeting individuals based on gender, occurring through digital platforms. It includes online harassment, image-based abuse, doxing, cyberstalking, impersonation, and gendered hate speech (Henry and Powell, 2015; Hameed et al., 2024). While definitions vary across legal and academic domains, DGV is broadly understood as gendered harm amplified by digital tools.

Foundational gender theorists offer key insights into the power structures that shape this violence. Judith Butler's (1990) concept of performativity shows how gendered norms are reinforced and policed in digital spaces. The repeated targeting of women and gender-diverse individuals reflects these performative structures. Rosalind Gill (2017) discusses digital sexualisation and "online misogyny" as key features of contemporary media culture. She highlights how platforms commodify women's bodies while enabling abuse. Donna Haraway's (1991) "cyborg" metaphor further explains the entanglement of bodies, machines, and gender politics. In DGV, identity and harm are mediated through digital assemblages, not just human actors.

The typology of digital violence varies across studies. Henry and Powell (2018) categorise image-based abuse, threats, and surveillance as core forms. Recent UN Women reports add layers of intersectionality, noting how race, caste, and sexuality compound these harms (UN Women, 2023). The Asia Foundation (2022) observes that women in South Asia face "culturally coded" abuse, often framed as moral correction. In Sri Lanka, Harasgama and Jayamaha (2023) found that digital harassment includes unsolicited explicit messages, image threats, and stalking, especially among university-aged women.

Sri Lankan research remains limited. Most studies are qualitative and small-scale (Inthusha and Kajananthan, 2023; Rajapaksha, 2023). There is a lack of longitudinal or comparative work. However, these studies confirm that DGV is normalised in youth discourse and seen as "part of being online." A lack of awareness and legal literacy hinders reporting.

Global reviews highlight three structural enablers of digital gender violence (DGV): platform design, weak law enforcement, and cultural permissiveness (Hameed et al., 2025). These same conditions are prevalent in Sri Lanka. Platforms such as WhatsApp, Facebook, and TikTok are frequently cited in complaints, yet platform accountability remains notably low (Search for Common Ground, 2024). The broader literature indicates a consensus that tech companies are rarely held responsible for the harms that occur on their platforms, and that existing legal frameworks often lag behind emerging digital behaviours (Commonwealth Secretariat, 2024; OECD, 2025).

From a sociolinguistic perspective, DGV also includes linguistic violence. Insults, threats, and shame are coded through gendered language. Labov (1972) argues that language serves as a means of social control. In DGV, attackers often use hybrid Sinhala-English phrases to mock, sexualise, or demean victims (Gunesekera, 2005). These discourses merit closer linguistic analysis.

Although digital gender violence (DGV) is often dismissed as "not real violence," scholars argue it has profound psychological and material effects (Henry and Powell, 2015). Victims frequently experience anxiety, engage in self-censorship, and withdraw from public life. In the Sri Lankan context, these impacts are often amplified by conservative norms around female behaviour and honour (Search for Common Ground, 2024).

In summary, DGV represents a complex form of harm shaped by digital architectures and entrenched gender ideologies. It manifests as both symbolic and material violence, impacting individuals linguistically and through legal frameworks. While Sri Lankan research largely aligns with global findings, there remains a critical need for stronger integration of theory, broader empirical scope, and comprehensive legal review.

3.2. Legal and Institutional Frameworks

Sri Lanka's legal response to digital gender violence remains limited, fragmented, and slow to adapt. Existing provisions are scattered across the Penal Code, the Computer Crimes Act (2007), and the newly introduced Online Safety Act (2024). However, these laws do not offer a comprehensive or gender-sensitive framework (Search for Common Ground, 2024; Jayasundara-Smits, 2022).

The Computer Crimes Act focuses mainly on unauthorised access, hacking, and data interference. While it criminalises "unauthorised use of information," it lacks specific references to image-based abuse, cyberstalking, or gendered hate speech. The Penal Code (as amended) criminalises criminal intimidation and sexual harassment, but enforcement in digital contexts is inconsistent and underdeveloped (Inthusha and Kajananthan, 2023; UN Women, 2023).

In response to growing public concern, the *Online Safety Act No. 09 of 2024* was passed (Amnesty International, 2024; Global Network Initiative, 2024). This Act establishes an Online Safety Commission tasked with regulating digital content and prosecuting harmful communications. Notably, Section 20 addresses online harassment, including the non-consensual sharing of private information, while other sections criminalise false statements and incitement. However, critics argue that the Act prioritises political control and censorship over genuine protection of vulnerable users, particularly women and minorities (Amnesty International, 2024; Freedom Forum, 2024; Global Network Initiative, 2024).

International bodies, such as UN Women and ITU, recommend that digital violence laws should include clear definitions, victim-centred approaches, and platform accountability (UN Women, 2021; ITU, 2023). Sri Lanka's legal framework falls short on all three counts. It lacks specific provisions for consent-based image sharing, digital impersonation, and algorithmic amplification of abuse.

Institutionally, Sri Lanka's response lacks dedicated cybercrime or gender violence units with sufficient technical or forensic capacity. Victims frequently have to lodge complaints at local police stations, where officers often lack adequate training in digital evidence and gender sensitivity (Search for Common Ground, 2024). This contributes to a high rate of non-reporting: studies indicate that female victims of online abuse frequently do not report incidents due to fear of stigma and perceived inaction by authorities (Search for Common Ground, 2024; WITNESS Blog, 2019).

In practice, enforcement is uneven. Police responses are often shaped by the victim's gender, age, and social status. Middle-class women in Colombo may access legal remedies more easily than rural women or LGBTQ+ individuals. Legal pluralism also complicates access to justice; in conservative communities, informal mediation is often preferred, sidelining victims' digital rights (Jayasundara-Smits, 2022).

Judicial outcomes are rare. Case law remains sparse. No published Sri Lankan precedent has clearly defined digital gender violence or addressed consent concerning private image circulation. This legal vacuum leaves most victims unprotected and discouraged from seeking redress.

Regional comparisons offer insight into legal responses to digital gender-based violence. India's *Information Technology Act* (Amendment 2008) includes Section 66E, which addresses privacy violations, and Section 67, which criminalises the publication or transmission of obscene content online. While the Act has been criticised for its vague provisions, it has nonetheless contributed to a growing body of case law on cyber-harassment. Similarly, Bangladesh's *Digital Security*

Act (2018) criminalises digital activities that violate privacy or dignity, including behaviour akin to revenge porn. However, the law has also raised concerns over free expression and due process. However, this legislation also faces significant criticism for its broad scope and potential for overreach (Human Rights Watch, 2020). Compared to these regional examples, Sri Lanka's legal tools for addressing digital gender violence remain underdeveloped and conspicuously lack a robust feminist framing.

In conclusion, Sri Lanka's legal and institutional frameworks offer limited and non-gender-sensitive protection against digital gender-based violence. The country lacks comprehensive laws tailored to the needs of women and marginalised groups online, as well as the enforcement capacity and survivor-centred procedures required to ensure justice. While the *Online Safety Act No. 9 of 2024* introduces new tools for addressing harmful online content, its effectiveness remains uncertain, particularly in the absence of robust accountability mechanisms, independent oversight, and trust-building with affected communities.

3.3. Policy Gaps and Governance Challenges

Sri Lanka's policy landscape on digital gender violence (DGV) reflects a reactive, fragmented, and underfunded approach. While the state acknowledges digital harms in general terms, there is no national policy that explicitly addresses gender-based abuse online. Current strategies are encompassed within broader frameworks for ICT, education, and women's protection. This lack of a targeted DGV policy undermines coordinated prevention and response mechanisms (UN Women, 2023).

The National Policy on Women (2010) and the National Plan of Action to Address Sexual and Gender-based Violence (2016–2020) offer limited references to digital abuse. Neither provides actionable strategies for DGV in contexts such as social media, image-based violence, or cyberstalking (Jayasundara-Smits, 2022). Despite evidence of growing digital risks, these frameworks remain outdated and largely disconnected from the technological realities facing young women and marginalised groups (The Asia Foundation, 2021).

There is also a governance gap in inter-agency coordination. The Ministry of Women and Child Affairs, the Ministry of Technology, and law enforcement agencies tend to operate in separate spheres. This institutional fragmentation can lead to inefficiencies in policy implementation, survivor support, and public awareness campaigns (Search for Common Ground, 2024). Enhancing cross-sectoral coordination is essential, though currently, such integrated efforts are limited.

Digital literacy remains underdeveloped across the population. Most awareness campaigns tend to focus on general internet safety rather than addressing gender-specific risks. Similarly, school curricula rarely cover topics such as online harassment, consent in digital spaces, or image privacy. Even within university settings, students have reported a lack of formal training on recognizing and reporting digital gender violence (Inthusha and Kajananthan, 2023; Harasgama and Jayamaha, 2023). This prevalent educational gap contributes to the normalisation of abuse and, consequently, hinders effective reporting.

At the community level, conservative gender norms further restrict victim disclosure. Women often face blame and reputational harm when digital abuse becomes public (Search for Common Ground, 2024; WITNESS Blog, 2019). LGBTQ+ individuals are particularly vulnerable due to legal invisibility and social stigma (WITNESS Blog, 2019). Policies, unfortunately, often do not adequately account for these intersectional barriers (Jayasundara-Smits, 2022; Search for Common Ground, 2024).

Platform governance in Sri Lanka is also weak. Global social media platforms often lack culturally responsive reporting systems, leading to struggles for victims in Sri Lanka to access platform moderators or receive timely responses. UN Women (2021) notes that users in South Asia frequently encounter a lack of content moderation in local languages, which significantly impedes the removal of harmful content. Furthermore, current policies do not effectively impose obligations on tech companies to cooperate with Sri Lankan law enforcement or provide data in cases of abuse (ITU, 2023).

In comparison, countries such as the Philippines and India have implemented digital literacy initiatives that include components focused on online safety. In the Philippines, the Digital Tayo program—a collaboration between Facebook Philippines and the Overseas Workers Welfare Administration (OWWA)—aims to educate citizens on online privacy, safety, digital discourse, and critical thinking through localised training modules (Facebook Philippines and Overseas Workers Welfare Administration, 2019). In India, the Cyber Surakshit Bharat initiative, launched by the Ministry of Electronics and Information Technology (MeitY), focuses on enhancing cybersecurity awareness among Chief Information Security Officers (CISOs) and IT professionals in government and public sector units through structured

workshops and capacity-building programs (Ministry of Electronics and Information Technology, 2018). While these efforts promote digital literacy and safety, Sri Lanka has yet to develop similarly large-scale initiatives with a dedicated gender-sensitive lens.

Finally, data collection remains limited in Sri Lanka. There is no centralised national database on cybercrime that is disaggregated by gender. Without such disaggregated data, it is challenging to assess the effectiveness of policies or allocate resources optimally and accurately. Most institutional reports tend to rely on anecdotal evidence or one-time surveys, which restrict the longitudinal tracking of trends (Search for Common Ground, 2024).

In summary, Sri Lanka's policy environment lacks a strategic, intersectional, and evidence-based approach to digital gender violence. The absence of coordinated governance, digital education, survivor support mechanisms, and platform regulation limits the impact of current measures. Effective governance must integrate gender-sensitive digital literacy, enforce platform accountability, and centre marginalised voices in policy-making.

3.4. Intersectionality and Vulnerable Groups

Digital gender violence (DGV) does not affect all individuals equally. An intersectional lens reveals how certain groups—such as LGBTQ+ persons, ethnic minorities, rural women, and youth—face compounded vulnerabilities online. These layers of identity shape exposure, experience, and response to digital harm (Crenshaw, 1991; Gill, 2017).

In Sri Lanka, patriarchal norms intersect with class, ethnicity, and sexual orientation to shape digital risks. Women from conservative or rural communities are more likely to face reputational harm, familial punishment, and social ostracism if targeted online. These consequences often silence victims before any legal or institutional remedy is sought (Inthusha and Kajananthan, 2023; Harasgama and Jayamaha, 2023).

LGBTQ+ individuals face a dual burden. They are disproportionately targeted and simultaneously invisible under Sri Lankan law. Same-sex relations remain criminalised under Section 365A of the Penal Code. As a result, LGBTQ+ victims of online abuse are often unwilling to report incidents due to fear of legal retaliation or outing (Human Rights Watch, 2023). Institutional protections for non-heteronormative identities are absent in digital policy and law.

Young women are among the most frequent targets of image-based abuse, threats, and online surveillance. Many face shaming linked to sexualised narratives or moral policing, often from peers or known individuals. This is further intensified on platforms like Facebook, TikTok, and WhatsApp, where networked harassment is common (Hameed et al., 2024; UN Women, 2021). In universities, online abuse has led to increased absenteeism, withdrawal from digital learning, and mental distress (Harasgama and Jayamaha, 2023).

Furthermore, women with disabilities encounter unique digital barriers. A report by ITU (2023) notes that global and regional ICT strategies rarely include accessible reporting tools or safety information for people with disabilities. No Sri Lankan policy or programme reviewed in the literature addresses this gap.

Digital access is also a privilege. Urban users may access privacy settings, digital literacy tools, and legal services more easily. Rural populations often lack the digital infrastructure, literacy, and institutional trust needed to seek redress. This divide reinforces pre-existing inequalities in access to justice and safety online (The Asia Foundation, 2021).

Intersectionality highlights how digital violence is not only gendered but also shaped by structural inequalities and identity-based discrimination. Policies and research that treat "women" as a homogenous group risk excluding the most marginalised. A truly effective response must consider the specific risks and needs of vulnerable groups across Sri Lankan society.

3.5. International Best Practices and Comparative Legal Approaches

Globally, states have begun to recognise digital gender violence (DGV) as a distinct and urgent policy concern. Countries with progressive legal responses provide valuable models for Sri Lanka. These include clear legal definitions, survivor-centred procedures, and digital literacy initiatives. Comparative analysis also highlights the risks of over-regulation and violations of freedom of expression (Hameed et al., 2024; Commonwealth Secretariat, 2024).

The Philippines enacted the Safe Spaces Act (2019), also known as the "Bawal Bastos Law." It explicitly covers online gender-based harassment. The law mandates educational institutions and private companies to provide complaint mechanisms. It also ensures rehabilitation for offenders and protection for victims (UN Women, 2021). The act integrates both punitive and preventative measures, including community-level education.

India's *Information Technology Act, 2000* (amended in 2008) includes Section 66E, which criminalises violations of privacy through the electronic capture or transmission of private images without consent. Section 67 penalises the publication and transmission of obscene content online. However, critics argue that enforcement remains inconsistent, and judicial interpretations of key terms vary (Bhangla and Tuli, 2021). India has also launched initiatives such as *Cyber Surakshit Bharat* to enhance cybersecurity and raise public awareness. Despite these efforts, the campaigns have offered limited attention to gender-specific harms and online abuse targeting women and marginalised groups.

Table 1 Key Legal Provisions Addressing Online Violence Against Women in India (Bhangla and Tuli, 2021)

Act	Clause	Details of the Offence This Provision Addresses	What Forms of Online VAW Can This Provision Help in Challenging?
IT Act	Section 66E	The capture and electronic transmission of images of private parts of a person, without his/her consent.	– Non-consensual circulation and malicious distribution of sexually explicit photographic and video material about an individual.
IT Act	Section 67	The publishing or transmission of obscene material in electronic form.	– Graphic sexual abuse on social media and blog platforms, including trolling. – Sending emails/social media messages with sexually explicit content and images to an individual, against his/her will.
IT Act	Section 67A	The publishing or transmission of sexually explicit content in electronic form.	– Graphic sexual abuse on social media and blog platforms, including trolling. – Sending emails/social media messages with sexually explicit content and images to an individual, against his/her will.
IT Act	Section 67B	The electronic publishing or transmission of material that depicts children in obscene, indecent, or sexually explicit manner.	– Circulation of child pornography.
IPC	Section 354A	Sexual harassment, including showing pornography against the will of a woman.	– Graphic sexual abuse on social media and blog platforms, including trolling. – Sending video and pictures with sexually explicit content and images to a woman, against her will.
IPC	Section 354C	Voyeurism, including watching or capturing images of a woman in a private act without consent, or sharing such images without her permission.	– Non-consensual production, circulation, and malicious distribution of sexually explicit photographic and video material about a woman.
IPC	Section 354D	Stalking: Following, contacting, or monitoring a woman online despite her disinterest.	– Cyberstalking. Only women are recognized as potential victims by the law.
IPC	Section 499	Criminal defamation leading to reputational harm.	– Though gender-neutral, it could be used by women bloggers and women on social media fighting slander and libel.
IPC	Section 507	Criminal intimidation through anonymous communication.	– Though gender-neutral, it could be used by women fighting online threats and harassment from anonymous users or trolls.
IPC	Section 509	Words, gestures, or acts intended to insult the modesty of a woman.	– Though not explicitly digital, it can be invoked in online sexual harassment and abuse cases.

In Australia, the eSafety Commissioner provides a strong institutional framework for online safety. The Online Safety Act 2021 enables swift removal of harmful content, including image-based abuse, and mandates that technology platforms adopt transparency protocols and user safety standards (Henry and Powell, 2022). The eSafety Commissioner operates independently, balancing enforcement with digital citizenship education.

Canada offers another instructive model. Under Section 162.1 of the Criminal Code, the non-consensual distribution of intimate images is criminalised, placing the burden of consent on the distributor rather than the subject. This legal framing reflects a feminist approach that centres the dignity and agency of victims (Citron, 2019).

The European Union's Digital Services Act (DSA), introduced in 2022, establishes legally binding obligations for large tech platforms to remove illegal content, perform risk assessments, and cooperate with regulators. While not gender-specific, the DSA addresses systemic harms such as misogyny and online hate speech by enforcing platform accountability (European Commission, 2022).

Sri Lanka can draw several lessons. First, laws must clearly define DGV. Vague or general provisions undermine enforcement. Second, institutional mechanisms—like an independent digital safety regulator—are crucial. Third, survivor-centred responses and education campaigns improve victim trust and social attitudes. Fourth, accountability should extend to tech platforms through duty-of-care models.

At the same time, Sri Lanka must avoid pitfalls seen in some jurisdictions. Broad laws, such as *Bangladesh's Digital Security Act (2018)* and *Pakistan's PECA (2016)*, have been criticised for enabling state surveillance and limiting freedom of expression. Feminist scholars caution that DGV laws should not be used as tools for moral policing or political suppression (Gill, 2017; Butler, 2004).

Effective legal reform must strike a balance between protection and rights. It must localise global best practices while responding to Sri Lanka's cultural, legal, and technological context.

4. Discussion

This chapter presents the findings from the literature review through the lens of feminist legal theory, digital governance, and intersectional gender analysis. It also evaluates how Sri Lanka's situation reflects and diverges from regional and global patterns of digital gender violence (DGV).

4.1. Normalisation of Digital Gender Violence

Digital Gendered Violence (DGV) in Sri Lanka is not isolated or sporadic. It reflects more profound structural inequalities in gender relations, public discourse, and digital platform design. As Butler (1990) suggests, gendered violence—including in digital forms—is a mechanism that polices normative identities. This is visible in how Sri Lankan women and LGBTQ+ persons are disproportionately targeted for expressing agency online.

Specifically, Harassment such as image-based abuse, impersonation, or moral policing operates as a form of social control. Research shows that this control is often justified through patriarchal narratives of honour, decency, and cultural propriety (Harasgama and Jayamaha, 2023; Rajapaksha, 2023). As Gill (2017) points out, such digital misogyny is a symptom of broader media cultures where women's bodies are simultaneously hypervisible and hyperregulated.

4.2. Gaps in Legal Interpretation and Protection

While Sri Lanka has introduced legal mechanisms, such as the Online Safety Act (2024), the findings suggest that its impact remains limited and controversial. The Act criminalises harmful online content but does so through vague language and discretionary powers (Amnesty International, 2024). These ambiguities may suppress free speech without adequately protecting victims.

The lack of clear definitions—particularly around consent, image-based abuse, or cyberstalking—creates enforcement challenges. By contrast, legal regimes in Canada and Australia specify non-consensual image sharing as a crime, with a burden of proof placed on the perpetrator (Henry and Powell, 2022; Citron, 2019). Sri Lanka's failure to explicitly address such offences reinforces a legal vacuum that leaves many forms of DGV unpunished.

4.3. Institutional and Policy-Level Fragmentation

Sri Lanka's institutional response is fragmented. Different ministries and law enforcement agencies operate in silos. Survivors often navigate a confusing system with limited technical capacity, gender sensitivity, or procedural consistency (Search for Common Ground, 2024) as the Asia Foundation (2021) and ITU (2023) note, a lack of inter-agency coordination is a common weakness in lower-middle-income digital governance.

Moreover, digital literacy programmes are not tailored to address gendered risks. The national curriculum overlooks crucial issues, including online consent, image privacy, and platform navigation for safety. Without early education and structured awareness, youth—particularly girls and gender-diverse individuals—remain uninformed and unprotected.

4.4. Platform Accountability and the Limits of Global Tech

Findings show that global platforms used heavily in Sri Lanka—such as Facebook, WhatsApp, and TikTok—are frequently implicated in DGV. However, they offer limited content moderation in Sinhala or Tamil (UN Women, 2023). Their reporting systems are inaccessible, opaque, and slow.

The lack of legally binding platform regulation allows these companies to deflect accountability. Jurisdictions like the EU (via the *Digital Services Act*) and Australia (via the eSafety Commission) now require transparency and user protection standards. Sri Lanka has no such binding obligations for tech companies, despite the heavy reliance on their infrastructure.

4.5. Vulnerable Populations and Intersectional Gaps

The review confirms that DGV disproportionately impacts individuals at the intersections of multiple vulnerabilities. LGBTQ+ persons face specific threats, including outing and legal risk due to criminalisation under Section 365A of the Penal Code (Human Rights Watch, 2023). Rural women often lack access to reporting channels or digital education. Victims with disabilities face accessibility barriers and invisibility in policy discourse (Hameed et al., 2024).

Crenshaw's (1991) framework of intersectionality remains highly relevant. Without inclusive data collection and participatory policy design, DGV interventions risk overlooking the most affected.

4.6. The Tension Between Protection and Control

Some legal provisions risk becoming tools for moral policing. Laws intended to protect may instead reinforce conservative ideologies. Butler (2004) and Gill (2017) caution that protective frameworks, if not grounded in rights-based language, may limit rather than expand digital agency for women and gender-diverse users.

Sri Lanka must therefore ensure that DGV interventions do not criminalise expression or reinforce surveillance-based governance. Protections must be specific, proportional, and centred on the lived realities of victims.

Table 1 Summary of Research Questions and Key Findings on Digital Gender Violence in Sri Lanka

Research Question	Summary of Findings
1. What are the main manifestations of digital gender violence in Sri Lanka?	Digital gender violence includes image-based abuse, cyberstalking, doxing, impersonation, and gendered hate speech. Women, LGBTQ+ individuals, and youth are most affected, especially on platforms like Facebook and WhatsApp.
2. How effective are existing legal and regulatory frameworks?	Sri Lanka's legal response remains fragmented. The Online Safety Act (2024) addresses some harms but lacks clear definitions and enforcement strength. Existing laws do not fully reflect consent-based or survivor-centred principles.
3. What gaps remain in policy, enforcement, and digital literacy?	There is no national DGV policy. Inter-agency coordination is poor, education on digital safety lacks gender sensitivity, and reporting systems are inaccessible. Digital literacy remains low in rural and marginalised communities.
4. Which international best practices can inform Sri Lankan responses?	Countries like Australia, Canada, and the Philippines offer models with clear definitions, regulatory oversight, and survivor-focused protections. Sri Lanka can adapt these while avoiding overregulation and censorship risks.

5. Conclusion

The findings of this review demonstrate that Digital Gender Violence (DGV) in Sri Lanka is a growing and under-addressed phenomenon. It is structurally rooted in both technological design and long-standing gender hierarchies. Online spaces are not neutral. Instead, they are extensions of offline power, where gendered abuse, surveillance, and objectification are routinely enacted.

Drawing on Judith Butler's (1990) theory of performativity, it becomes clear that digital harassment is a mechanism through which femininity, queerness, and resistance are policed. Haraway's (1991) cyborg metaphor reminds us that digital harm is embodied. Sri Lankan women, LGBTQ+ individuals, and other marginalised groups experience this

violence not as abstract data, but as lived trauma. These experiences are further shaped by sociocultural norms, class, age, and geography.

Digital platforms act as accelerators of violence. Their algorithms prioritise visibility and engagement, often at the expense of safety. While individuals may initiate abuse, its persistence is enabled by the inaction of platforms and the failures of law and policy.

This paper aimed to examine how digital gender violence manifests in Sri Lanka, how it is addressed legally and institutionally, and how international models might guide reform. The review focused on the intersections between law, gender, technology, and policy. It highlighted emerging trends, critically evaluated legal texts, assessed policy responses, and analysed institutional and platform accountability frameworks.

5.1. Recap of Key Findings and Contributions

5.1.1. The review identified four central findings:

First, DGV in Sri Lanka includes image-based abuse, cyberstalking, doxing, impersonation, and gendered hate speech. These acts disproportionately affect women and LGBTQ+ persons, especially on social media platforms. Victims frequently experience shame, reputational damage, and mental distress.

Second, legal responses are fragmented. While the Online Safety Act (2024) introduces new offences, its language remains vague, and its enforcement mechanisms are politically contested (Amnesty International, 2024). Existing statutes, such as the Computer Crimes Act and Penal Code, do not clearly define gendered digital harms or incorporate consent-based standards.

Third, policy responses lack coordination and inclusivity. There is no national policy dedicated to DGV. Ministries and enforcement agencies operate in isolation. Digital literacy programmes do not engage with gender-specific risks. Public trust in reporting systems remains low, particularly among rural women, youth, and queer users.

Fourth, comparative models—such as Australia's eSafety Commission, Canada's non-consensual image law, and the EU's Digital Services Act—offer viable frameworks for reform. These models prioritise platform regulation, user safety, and survivor-centred legal definitions. However, such models must be localised to the Sri Lankan context.

This review contributes a comprehensive and critical synthesis of literature, policy, and law on DGV in Sri Lanka. It bridges theoretical insights with applied analysis. It also identifies gaps in regulation, education, and research.

5.2. Practical Implications

5.2.1. The findings have implications for multiple stakeholders.

Policymakers must adopt a standalone digital gender violence policy. This policy should include intersectional risk assessments, preventive strategies, and survivor support systems. It must mandate training for police, judiciary, and educators.

Lawmakers should reform existing laws to include precise definitions of DGV. These laws must reflect international standards on consent, image rights, and online stalking. Judicial training and survivor protection mechanisms should accompany these reforms.

Educational authorities must embed digital literacy, consent, and gender equality into school and university curricula. These initiatives should be accessible in Sinhala and Tamil, and address rural and marginalised communities.

Technology platforms must be held accountable through clear duty-of-care obligations. Reporting tools should be multilingual, accessible, and responsive. Transparency in content moderation and data sharing with law enforcement is essential.

Civil society organisations must continue to advocate for digital rights, platform regulation, and law reform. Partnerships between feminist organisations, disability groups, and LGBTQ+ networks can ensure inclusive policy outcomes.

Researchers should focus on under-studied groups, such as sex workers, disabled persons, and rural communities. Mixed-method studies and longitudinal tracking are needed. Partnerships with global organisations can support comparative research.

Donors and international agencies should support locally led initiatives focused on digital safety, legal literacy, and survivor advocacy. These efforts should foreground feminist and intersectional values, resisting one-size-fits-all approaches.

5.3. Limitations

5.3.1. This review faces several limitations.

First, much of the Sri Lankan literature is qualitative and small-scale. Quantitative data, particularly on incidence and prevalence, remains sparse. This limits generalizability.

Second, there is limited publicly available case law related to digital gender violence. Judicial responses are often undocumented or inaccessible, constraining legal analysis.

Third, while the review incorporates multiple disciplines, it does not deeply examine technical architecture (e.g., algorithmic bias or encryption) that facilitates or conceals DGV. Further interdisciplinary work is needed to engage engineers and data scientists.

Fourth, some international frameworks reviewed may not translate seamlessly into Sri Lanka's legal or cultural context. Localisation and cultural sensitivity are necessary in adapting models.

Fifth, grey literature was excluded in order to prioritise verifiability. While this ensured academic rigour, it may have omitted relevant practitioner insights or community experiences not published in formal channels.

Despite these limitations, the review provides a strong foundation for future inquiry and action. It positions DGV as a human rights, legal, and social justice issue that demands urgent, informed, and inclusive solutions.

Compliance with ethical standards

Disclosure of conflict of interest

The author declares no conflict of interest.

Funding

No external funding was received for the preparation of this manuscript.

Data Availability Statement

No datasets were generated or analysed during the current study.

References

[1] Amnesty International. (2024, February 2). Sri Lanka: New Online Safety Act a major blow to freedom of expression. https://www.amnesty.org/en/latest/news/2024/01/sri-lanka-online-safety-act-major-blow-to-freedom-of-expression/

[2] Bhangla, A., and Tuli, J. (2021). A study on cyber crime and its legal framework in India. International Journal of Law Management and Humanities, 4(2), 493–504. http://doi.one/10.1732/IJLMH.26089 ijraset.com+8

[3] Butler, J. (1990). Gender trouble: Feminism and the subversion of identity. Routledge.

[4] Butler, J. (2004). Undoing gender. Routledge.

[5] Citron, D. K. (2019). Hate crimes in cyberspace. Harvard University Press.

[6] Crenshaw, K. (1991). Mapping the margins: Intersectionality, identity politics, and violence against women of color. Stanford Law Review, 43(6), 1241–1299. https://doi.org/10.2307/1229039

[7] European Commission. (2022). The Digital Services Act package. https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

[8] Facebook Philippines, and Overseas Workers Welfare Administration. (2019, May 11). Facebook rolls out Digital Tayo program. BusinessMirror. https://businessmirror.com.ph/2019/05/11/facebook-rolls-out-digital-tayo-program/

[9] Gill, R. (2017). The affective, cultural and psychic life of postfeminism: A postfeminist sensibility 10 years on. European Journal of Cultural Studies, 20(6), 606–626. https://doi.org/10.1177/1367549417733003

[10] Global Network Initiative. (2024, February 19). GNI statement on Sri Lanka's Online Safety Act. https://globalnetworkinitiative.org/sri-lankas-online-safety-act-a-year-in-review-and-framework-for-reform/

[11] Gunesekera, M. (2005). The postcolonial identity of Sri Lankan English. Vijitha Yapa Publishers.

[12] Hameed, S., Tyabashe-Phume, B., Tunggal, E., Hunt, X., Ned, L., and Soldatić, K. (2024). Technology-facilitated gender-based violence against women with disabilities in low- and middle-income countries: A scoping review protocol. BMJ Open, 14(8), e093988. https://doi.org/10.1136/bmjopen-2024-093988

[13] Harasgama, K. S., and Jayamaha, S. (2023). Online harassment in Sri Lanka: A thematic analysis. Social Sciences, 12(3), 176. https://doi.org/10.3390/socsci12030176

[14] Haraway, D. J. (1991). Simians, cyborgs, and women: The reinvention of nature. Routledge.

[15] Henry, N., and Powell, A. (2015). Embodied harms: Gender, shame, and technology-facilitated sexual violence. Violence Against Women, 21(6), 758–779. https://doi.org/10.1177/1077801215576581

[16] Human Rights Watch. (2023). "All five fingers are not the same": Discrimination on grounds of gender and sexual orientation in Sri Lanka. https://www.hrw.org/

[17] Information and Communication Technology Agency (ICTA). (2018). National digital policy for Sri Lanka: Towards a digital nation. Government of Sri Lanka. https://www.icta.lk/

[18] Information Technology Act, No. 21 of 2000 (India), as amended by the Information Technology (Amendment) Act, 2008.

[19] International Telecommunication Union (ITU). (2023). Guidelines for developing legal frameworks to address online gender-based violence. https://www.itu.int/

[20] Inter-Parliamentary Union. (2025, March 25). 60% of women MPs from Asia-Pacific report online gender-based violence. https://www.ipu.org/news/press-releases/2025-03/60-women-mps-asia-pacific-report-online-gender-based-violence

[21] Inthusha, K., and Kajananthan, R. (2023). Cyberbullying among university students: A study on Sri Lankan universities. Journal of Business Studies, 10(2), 59–73. https://doi.org/10.4038/jbs.v10i2.98

[22] Jayasundara Smits, S. (2022). Politico religious extremism and violence against women in Sri Lanka (EGV Sri Lanka) [Report]. IMADR, supported by the European Union. International Institute of Social Studies, Erasmus University Rotterdam. Retrieved from https://pure.eur.nl/ws/portalfiles/portal/77620911/EGV_Sri_Lanka_JayasundaraSmits.pdf

[23] Labov, W. (1972). Sociolinguistic patterns. University of Pennsylvania Press.

[24] Ministry of Electronics and Information Technology. (2018, January 19). MeitY launches Cyber Surakshit Bharat to strengthen cybersecurity. Press Information Bureau, Government of India. https://pib.gov.in/PressReleasePage.aspx?PRID=1517238

[25] OECD. (2025). Mapping policy responses to technology-facilitated gender-based violence in the G7 countries. OECD Public Governance Policy Papers, No. 75. OECD Publishing. https://doi.org/10.1787/b0887189-en

[26] Parliament of the Democratic Socialist Republic of Sri Lanka. (2024). Online Safety Act, No. 9 of 2024 [Act]. Retrieved from https://www.parliament.lk/uploads/acts/gbills/english/6311.pdf

[27] Rajapaksha, N. (2023, December). Cyber sexual and gender based violence in Sri Lanka: A legal gap analysis [Report]. Search for Common Ground. Retrieved from https://www.sfcg.org/wp-content/uploads/2023/11/CitW_Gap_Analysis_2023_SFCG.pdf

[28] Search for Common Ground. (2024). Unveiling digital realities: Tackling gendered drivers of the conflict and exclusion in cyberspace. https://www.sfcg.org/wp-content/uploads/2024/02/Unveiling-Digital-Realities-Final.pdf

[29] The Asia Foundation. (2021). Optimising screening and support services for gender-based violence and trafficking in persons victims: Sri Lanka [Report]. The Asia Foundation and Centre for Poverty Analysis. Retrieved from https://asiafoundation.org/wp-content/uploads/2024/08/Sri-Lanka_Optimizing-Screening-and-Support-Services-for-Gender-Based-Violence-and-Trafficking-in-Person-Victims.pdf

[30] UN Women. (2021). Online and ICT-facilitated violence against women and girls during COVID-19. https://www.unwomen.org/

[31] United Nations Population Fund. (n.d.). Preventing technology-facilitated gender-based violence (TF GBV). Retrieved June 27, 2025, from https://www.un.org/digital-emerging-technologies/sites/www.un.org.techenvoy/files/GDC-Submission_UNFPA.pdf

[32] United Nations Women. (2021). Online and ICT-facilitated violence against women and girls during COVID 19 [Policy brief]. UN Women. https://doi.org/10.18356/b3f5cc80-en

[33] United Nations Women. (2023). Creating safe digital spaces free of trolls, doxing, and hate speech [Explainer]. UN Women. Retrieved from https://www.unwomen.org/en/news-stories/explainer/2023/11/creating-safe-digital-spaces-free-of-trolls-doxing-and-hate-speech

[34] WITNESS Blog. (2019, September 24). Cyber-violence against the marginalised in Sri Lanka. https://blog.witness.org/2019/09/cyber-violence-groundviews-sri-lanka/