

Digital Spaces, Structural Inequalities: Rethinking TFGBV in South Asia's Legal and Socio-Cultural Context

Sadichchha Silwal  and Sanjina Kshetri 

Advocate

Article Info.

Corresponding Author

Sadichchha Silwal

Email

sadii.silwal@gmail.com

Article History

Received: 30 April 2026

Accepted: 1 July 2026

Published: 31 July 2026

How to Cite this Article

Silwal, S., & Kshetri, S. (2026). Digital Spaces, Structural Inequalities: Rethinking TFGBV in South Asia's Legal and Socio-Cultural Context. *The Informal: South Asian Journal of Human Rights and Social Justice*, 3 (1), 29-46.

Abstract

This article explores the growing prevalence of technology-facilitated gender-based violence (TFGBV) in South Asia within the context of rapid digital expansion and persistent structural inequalities. While increased internet penetration across Nepal, India, Pakistan, Bangladesh, and Sri Lanka has enabled greater access to information, freedom of expression, and economic participation, it has simultaneously amplified gendered forms of harm in digital spaces. Manifestations of TFGBV, including cyberstalking, doxxing, image-based abuse, and online sexual harassment, reflects a spillover of entrenched patriarchal violence into digital spaces rather than a completely new phenomenon. Adopting a triangulated qualitative methodology, the study combines doctrinal legal analysis with a comparative and socio-legal approach to assess the adequacy of legal frameworks and their enforcement mechanisms. The findings suggest that legal responses across the region remain fragmented, morality-driven, and heavily reliant on criminalization, often failing to address the consent-based, intersectional, and rapidly evolving nature of digital harms. Legal ambiguities, weak enforcement mechanisms, and limited institutional capacity further widen the gap between formal protections and the lived realities of survivors. The article further underscores how socio-cultural barriers, including victim-blaming attitudes, honor-based social norms, and unequal access to digital technologies, restrict reporting and impede access to justice. It argues that TFGBV not only inflicts harm on individuals but also restricts women's participation in public and digital spaces, thereby undermining democratic engagement and civic inclusion. It calls for a shift toward survivor-centered, rights-based approaches integrating legal reform, platform accountability, digital literacy, and broader processes of social transformation.

Keywords: technology facilitated gender based violence, socio legal analysis, south asia, structural inequality, survivor centered justice

Introduction

The development of computers and the internet since the mid-twentieth century has fundamentally transformed contemporary societies. Technological innovation has profoundly transformed society-

influencing daily life, culture, politics, and economics. It has reshaped patterns of communication, governance, and social interaction, giving rise to an increasingly interconnected digital world. Across South Asia, internet penetration

has expanded rapidly, driven by the widespread availability of affordable smartphones and mobile data services. As of late 2025, internet penetration in India stood at approximately 70 percent, with over 1.03 billion users, compared to 644 million users in 2021 (Kemp, 2025a). In early 2026, Pakistan's internet penetration rate was 45.6 percent with approximately 117 million internet users (Kemp, 2025b). During the same period, Sri Lanka stood at 59.7 percent, representing 13.9 million individual users, (Kemp, 2025c), while Bangladesh remained at 47 percent with 82.8 million users (Kemp, 2025d). In Nepal, the internet penetration rate stood at 56 percent with approximately 16.6 million internet users (Kemp, 2025e), with the information technology (IT) sector contributing around 1.7 percent of the national GDP (National Statistics Office, 2025). With this, the internet has emerged as a critical platform for communication, participation, and the exercise of fundamental freedom. According to the UNFPA, digital technologies enabled women to access information, amplify their voices, advocate for required change, and pursue economic opportunities (UNFPA, 2024).

Alongside these advances, the misuse of digital tools has also increased, disproportionately targeting women and girls in the form of technology-facilitated gender-based violence (TFGBV). While enabled by contemporary technologies, TFGBV represents an evolution of traditional forms of gender-based violence (GBV), extending them into online and digitally mediated spaces. TFGBV encompasses a broad spectrum of abusive behaviors such as cyberstalking, doxxing, image-based abuse, sextortion, online sexual harassment, and cyberbullying. This form of GBV goes beyond geographical boundaries, infiltrating both private and public spheres, and often blurring the distinction between online and offline harms. In many instances, digital abuse serves as a precursor to or facilitator of offline violence, including stalking, physical assault, and in extreme cases, femicide.

The scale and prevalence of TFGBV has become a growing global concern. According to UN women, millions of women worldwide

experience technology-facilitated violence each year (UN Women, 2025). UN Women estimates indicate that between 16 and 58 percent of women globally have experienced some form of online or technology-facilitated violence (UN Women, 2022). Regional data further underscores the widespread nature of the problem. In Arab States, approximately 60 percent of female internet users report experiencing online violence (UN Women, 2021). Research conducted across twelve countries in Eastern Europe and Central Asia found that over 50 percent of women aged 18 and above had experienced some form of technology-facilitated abuse (UN Women, 2024). Similarly, a five-country study in Sub-Saharan Africa reported 28 percent of women had encountered online violence (Iyer et al., 2020), while a survey conducted across countries in Europe and the United States found 23 percent of women aged 18-55 had experienced at least one form of online abuse or harassment (Amnesty International, 2017).

These challenges are particularly significant in South Asia. Although countries in the region are rapidly expanding their digital infrastructure and online populations (Singh & Ferraz, 2023), they continue to undergo complex political, economic, and institutional transitions. For instance, Nepal continues to navigate post-conflict democratic consolidation amid recurring political instability; Sri Lanka is recovering from a protracted economic crisis; Bangladesh has experienced significant economic volatility amid political suppression; Pakistan continues to face recurring volatile politics; and India's democratic expansion with rising authoritarian tendencies are all pointing towards a similar trend in South Asia i.e. transitional period. This volatile intersection of political flux and rapid digitization creates a precarious environment where technological advancement frequently outpaces the evolution of legal, regulatory, and institutional safeguards. As a result, women and marginalized groups remain particularly vulnerable to emerging forms of digital harm.

The challenges posed by TFGBV are further exacerbated by deeply rooted social inequalities. Across South Asian countries, patriarchal social

structures continue to shape gender relations and influence women's access to opportunities, resources, and justice. These inequalities are reinforced in the forms of discrimination based on caste, ethnicity, religion, class, disability, and other social identities. Every nation in the region is carrying out the burden of patriarchal norms, weak regulatory frameworks, and bears the spectrum of this burden in its societal practices. Within this context, TFGBV is often dismissed as a normal digital byproduct or as a mere cost of women's visibility in public spaces. Such perceptions obscure the structural nature of the problem. Rather than constituting a distinct form of violence detached from social realities, TFGBV reflects the amplifications of existing patterns of discrimination, control, harassment, and violence into digital spaces. Consequently, online environments frequently reproduce and reinforce the same gendered hierarchies that constrain women's participation in social, political, and economic life.

Against this backdrop, this paper aims to understand the ongoing scenario of South Asia where the undergoing rapid digital transformation, legal loopholes and deeply entrenched gender inequalities are driving the experiences of women in the digital space. This paper critically investigates TFGBV in South Asia through three interrelated analytical lenses: first, the conceptualization and recognition of digital harms within regional legal frameworks; second, the adequacy of current legal responses to emerging technological threats, including artificial intelligence (AI) enabled harms such as deepfakes; and third, the socio-legal barriers that impede reporting, accountability, and access to justice for survivors.

Employing a triangulated qualitative methodology, the study combines doctrinal analysis of legislation across Nepal, India, Pakistan, Sri Lanka and Bangladesh with a comparative regional review. These findings are further contextualized through a socio-legal analysis, contrasting statutory provisions with empirical data on survivor experiences, enforcement gaps, and institutional responses. By examining the relationship between law, technology, and social structures, the article

seeks to illustrate the persistent gap between formal legal guarantees and the lived realities of women experiencing technology-facilitated violence in South Asia.

Conceptual Framework

TFGBV represents an evolving and multifaceted form of harm that emerges at the intersection of digital technologies and structural gender inequalities. According to the UNFPA, TFGBV refers to "*an act of violence perpetrated by one or more individuals that is committed, assisted, aggravated and amplified in part or fully by the use of information and communication technologies or digital media against a person on the basis of their gender*" (UNFP, n.d.). Similarly, UN Women conceptualizes Technology Facilitated Violence Against Women (TFVAW), a term often used *interchangeably with TFGBV*, as "*any act committed, assisted, aggravated, or amplified by the use of ICTs or other digital tools, that results in or is likely to result in physical, sexual, psychological, social, political, or economic harm, or other infringements of rights and freedoms*" (UN Women & World Health Organization, 2022). These definitions emphasize that digital violence is not merely a technological phenomenon but a manifestation of broader systems of gender inequality and discrimination that frequently intersect with race, ethnicity, class, gender identity, sexual orientation, and disability.

Distinguishing TFGBV from broader categories of cybercrime is conceptually crucial. While acts such as cyberstalking, doxxing, online harassment, image-based sexual abuse, and gendered disinformation are often addressed within the broader category of cybercrime, TFGBV differs in its inherently gendered nature. Unlike conventional cybercrime, which is generally concerned with unauthorized access, fraud, or digital security, TFGBV targets individuals based on gender and exploits existing social hierarchies and structural vulnerabilities. Understanding TFGBV therefore requires moving beyond technologically deterministic perspectives that view digital platforms as neutral tools that are merely misused. Instead, it necessitates an examination of how technology interacts with

pre-existing social relations, power structures, and systems of discrimination.

Feminist legal scholars provide an important theoretical foundation for understanding this relationship. MacKinnon (1989) argues that the law often reproduces and legitimizes gendered hierarchies, portraying women as inherently inferior or dependent and embedding masculinist values into legal systems. Such critiques are particularly relevant in South Asia, where gender inequalities are reinforced not only through formal legal frameworks but also through deeply rooted cultural norms that privilege male authority and constrain women's autonomy (The Annapurna Express, 2025). Women's struggles derive not merely from isolated injustices but from entrenched socio-cultural structures that normalize inequality as normative rather than exceptional. Even celebrated moments in technology leadership reveal persistent gendered expectations. For instance, the public debate in 2012 surrounding the pregnancy of a prominent tech CEO underscored how questions of whether one can "have it all" are disproportionately directed at women and rarely at men, thereby reinforcing persistent biases about gender, work, and value in technology-shaped spaces (ABC7, 2012). Similarly, in 2021, a software engineer recounted returning from maternity leave only to find her new-mother status perceived as a "big problem" by certain big tech teams, exposing tension between the industry's self-image of flexibility and its gendered practices (Kate, 2021). During Nepal's March 2026 elections, women candidates were subjected to online abuse targeting their bodies, pregnancy and reproductive status as evidence of supposed unfitness for political office, with commentators urging them to "stay at home" (Chand, 2026). Such attacks illustrate how digital spaces reproduce longstanding gender hierarchies, using women's physicality and prescribed roles to question their participation in public life.

Earlier feminist scholarship highlighted how the private lives of women were neglected in the law and denied appropriate legal recognition. Today, however, the dividing line between private and public spheres has become increasingly narrower. Women now articulate their identities

and experiences through social media, often facing resistance from traditional social norms that show what, how and when women express themselves. TFGBV extends this dynamic, as private interactions are weaponized in public platforms—for instance, leaked private chats following a rejected romantic proposal, reflecting the persistence of patriarchal norms.

Digital environments, often designed with masculinist assumptions, exacerbate these harms by enabling surveillance and control while framing violations as individuals rather than systemic. Moreover, the economic architecture of social media platforms rewards engagement and amplifies provocative, emotionally charged content, allowing misogynistic and hyper-masculine narratives to thrive through algorithmic promotion and monetized virality (Agyare, 2025). The convergence of cultural patriarchy, algorithmic bias, and digital capitalism (Scasserra, 2024) thus reinforces gender hierarchies and accelerates the normalization of TFGBV, particularly in socioeconomically fragile contexts (Renström & Bäck, 2024). In such settings, young people are especially vulnerable, consuming algorithmically curated content that structurally reproduces patriarchy norms.

Comparative Legal Frameworks: Criminalization as Primary Response

South Asian countries, particularly Nepal, India, Pakistan, Bangladesh, and Sri Lanka, have adopted laws to address TFGBV, though these responses remain predominantly a criminalization-focused approach. This section outlines key legislative measures across these five South Asian countries that aim to respond to TFGBV.

Nepal

The Constitution of Nepal (2015) guarantees right to equality under Article 18, explicitly prohibiting gender discrimination, and protects privacy under Article 28, including personal data, correspondence, and character. Freedom of expression and communication is safeguarded under Articles 17 and 19, subject to reasonable restrictions for public morality or harmony. Article 21 guarantees victims of crime the right to justice,

including social rehabilitation, compensation, and information about the investigation and legal proceedings. Article 38(3) prohibits violence or exploitation against women on grounds of religion, social, cultural tradition, practice or on any other grounds, entitling victims to compensation. These provisions theoretically safeguard against TFGBV as violations of dignity and equality, yet digital application remains limited, with courts rarely interpreting them expansively for online gender harms.

The primary statutory framework relies on the outdated Electronic Transactions Act (2006) (amended in 2015), particularly Section 47, which penalizes publication or display of electronic materials contrary to public morality, decency, or spreading hate or jealousy with fines up to NPR 100,000 and/or up to 5 years imprisonment. This vague, morality-oriented provision has been applied to cyber harassment, non-consensual image sharing, defamation, and obscene content against women, but risks criminalizing victims themselves. Supplementary provisions in the National Penal Code (2017) include Section 121 (obscenity), Section 224 (sexual harassment), and Section 225 (child sexual harassment, including offenses committed through electronic media). However, this morality-based framing often shifts focus from consent to content, imposing evidentiary burdens on survivors. Section 66(3) of the Act Related to the Rights of Children (2018) offers specific protections for minors but remains significantly underutilized.

The existing legal framework governing cybercrime remains notably limited in scope, as it fails to explicitly recognize and address emerging forms of TFGBV, such as sextortion, deepfakes, cheapfakes, and online grooming. There is no dedicated statutory provision to address non-consensual dissemination of intimate images, commonly referred to as “revenge pornography”. Data protection under the Privacy Act (2018) (Individual Privacy Act, 2018) remains fragmented and insufficiently gender responsive. Importantly, existing laws do not adequately account for the intersectional dimensions of TFGBV, which disproportionately affect women and girls from

marginalized communities, including Dalit and Madhesi individuals as well as women in public and professional spheres. These gaps underscore the absence of a comprehensive, inclusive, and gender-responsive legal approach.

The long-overdue Information Technology and Cyber Security Bill (2025) seeks to modernize Nepal’s cybercrime framework by addressing digital records, cybersecurity, and emerging technological threats, but has been subject to significant criticism. There have been concerns raised regarding its vague provisions, which risk undermining freedom of expression; lack of a gender-sensitive perspective, and absence of survivor-centered mechanisms. This failure underscores systemic delays in reform. Moreover, following the dissolution of Parliament in the aftermath of the Gen-Z protests, the bill has effectively lapsed, further delaying much-needed legal reform.

Critically, existing legal provisions remain grounded in morality-based standards emphasizing notions such as “public decency” and “social harmony” rather than principles of gender justice. This approach not only enables potential misuse of the law, such as victim-blaming and retaliatory litigation against survivors, but also fails to address underlying structural drivers of online misogyny. The increasing number of complaints related to violence against women in digital spaces, around 54 cybercrime cases lodged per day (Nepal Police, 2023) and over 18,000 cases in FY 2025/26 (Nepal Police n.d.), highlight systemic shortcomings. Despite rising reports, prosecution rates remain low due to evidentiary challenges, limited forensic capacity, inadequate training among law enforcement personnel, resource constraints, and weak cooperation from digital platforms. These institutional challenges, coupled with persistent social stigma, contribute to significant underreporting and impede access to justice for survivors.

India

The Indian constitutional framework offers foundational protections against GBV, including TFGBV, though their application remains uneven.

Articles 14 and 15 of the Constitution guarantee equality before the law and prohibit discrimination on grounds of sex, while Article 21, expansively interpreted by the Supreme Court in *Justice K.S. Puttaswamy (Retd.) v. Union of India* (2017), incorporates the right to privacy and thereby underpins protections against non-consensual digital intrusions.

The primary statutory instruments remain the Information Technology Act (2000) (as amended in 2008) and complementary provisions of the Indian Penal Code (1860) (IPC), now largely subsumed under the Bharatiya Nyaya Sanhita, 2023 (BNS), effective from July 2024. Under the Information Technology Act, Section 66E criminalizes violation of privacy through the capture, publication, or transmission of private images without consent. Sections 67, 67A, and 67B address the publication or transmission of obscene material, sexually explicit content, and child pornography in electronic form. Parallel provisions in the BNS include Section 75 (sexual harassment, formerly IPC 354A), Section 77 (voyeurism, formerly 354C), Section 78 (stalking, including cyberstalking, formerly 354D), and Section 79 (acts intended to insult the modesty of woman, formerly 509). These provisions are frequently invoked in TFGBV cases involving non-consensual intimate imagery, cyberstalking, and online harassment. (Khan et al., 2025; The Digital Personal Data Protection Act, 2022)

The Digital Personal Data Protection Act (2023) (DPDP Act), its Rule enacted in November 2025, introduces a consent-based framework for the processing of digital personal data, including obligations for data fiduciaries regarding security, breach notification, and individual rights. However, its scope remains general and does not explicitly address gendered digital harms such as revenge pornography or deepfake abuse, leaving significant gaps in survivor-centric remedies.

Regulatory developments have sought to address emerging threats, particularly synthetic media. In February 2026, the Ministry of Electronics and Information Technology (MeitY) modified the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules

(2026), introducing obligations for intermediaries regarding “synthetically generated information” (SGI), defined as audio-visual content artificially or algorithmically created or altered to appear indistinguishable from reality (explicitly encompassing deepfakes) (Bhatt Joshi Associates, 2026). Requirements include mandatory labelling of SGI, embedding provenance metadata, quarterly user notifications on misuse liabilities, expedited takedown timelines for flagged harmful content (e.g., nudity, impersonation, or non-consensual intimate imagery), and due diligence to prevent dissemination of misleading or privacy-violating material. While proactive, critics note risks of overbreadth and potential constrictive effects on free expression.

Despite this evolving architecture, Indian TFGBV laws remain predominantly morality-oriented, centered on notions of “obscenity” and “modesty”, rather than explicitly survivor-justice or consent-based. This framing facilitates selective enforcement, survivor-blaming, and weaponization of provisions against victims themselves, e.g., through counter-cases or threats of prosecution under obscenity laws. The existing data shows the scale of the crisis: National Cyber Crime Reporting Portal (NCRP) figures show cybercrime complaints against women rose from 48,335 in 2024 to 76,657 in 2025, a 58 percent increase in one year, with obscene content (37,743 cases) and sexually explicit acts (19,703 cases) dominating reports (Storyboard18, 2026). Between 2020 (22,188 cases) and 2024(48,475 cases), online crimes against women surged by 118.4 percent (Francis A.M., 2025). Deepfake-specific abuse has escalated dramatically, with reports indicating a 900 percent growth in volume and 98 percent of explicit deepfakes targeting women (Shinde, 2026). Underreporting remains rampant; one study estimates that 62 percent of deepfake abuse cases involving women go unreported due to stigma and fear of retaliation (Shinde, 2026).

Overall, while India has a basic legal framework to address TFGBV, its reliance on morality-based approach, punitive laws, fragmented implementation, and weak enforcement fail to meet survivors’ realities. Reforms such as consent-

based offences for image abuse, mandatory gender-sensitization, stronger integration with the DPDP Act, and survivor-led monitoring of the 2026 IT Rules are essential for advancing meaningful justice.

Pakistan

Article 25 of the Constitution of Pakistan guarantees equality of citizens before the law and prohibits discrimination on the basis of sex, while Article 14(1) declares the dignity of man and the privacy of the home to be inviolable. Although the limited judicial pronouncements have extended the right to privacy to personal data and digital contexts, enforcement in online spaces remains weak. In practice, broad cyber laws have often been deployed to suppress dissent rather than safeguard against gendered online harms, creating a persistent tension between expressive freedoms and the need to curb digital violence.

The cornerstone of Pakistan's cybercrime legislation is the Prevention of Electronic Crimes Act (PECA) (2016). Key provisions of the Act invoked in TFGBV cases include Section 20 (offences against the dignity of a natural person), Section 21 (offences against the modesty of a natural person, including minors), Section 24 (criminalizes cyberstalking), and Section 22 (prohibits child pornography). These are frequently supplemented by provisions from the Pakistan Penal Code (1860) (PPC) such as Section 416 (cheating by personation) and Section 500 (defamation). Although these sections provide means to address non-consensual sharing of intimate images, online harassment, and stalking, the framework remains heavily oriented toward notions of "dignity" and "modesty" rather than explicit consent, survivor autonomy, or recognition of misogynistic intent.

In January 2025, Parliament passed the Prevention of Electronic Crimes (Amendment) Act (2025), introducing significant institutional changes. The amendments established the Social Media Protection and Regulatory Authority (SMRA or SMPRA) with broad powers to regulate unlawful or offensive content, issue 24-hour takedown orders, enlist and oversee social media platform compliance, and impose sanctions or shutdown of

non-compliant services (Amnesty International, 2025). A three-tier complaints mechanism was created, involving the Authority, a Council, and appellate Tribunals, with appeals bypassing High Courts directly to the Supreme Court. Additional provisions criminalized the dissemination of "false or fake information," with penalties of up to three years imprisonment. While intended to address disinformation, these provisions have been widely criticized for their vagueness and potential misuse to silence victims or critics reporting TFGBV. Human rights organizations argue that the amendments expand state surveillance, enable arbitrary censorship, and prioritize content control over survivor-centric protections, particularly affecting women journalists and activists who risk countersuits for "spreading false information" when documenting abuse.

Pakistan currently lacks a comprehensive data protection law tailored to digital harms or gender-based violence. A draft Personal Data Protection Bill has been under consideration since 2023 (Privacy International, 2023) but is yet to be enacted. This gap leaves survivors of image-based abuse, doxxing, and deepfakes without robust consent-based safeguards or obligations on data fiduciaries, exacerbating vulnerabilities in the absence of explicit integration with TFGBV remedies. In March 2026, the Ministry of Human Rights, with UNDP support, launched Pakistan's first National Strategy to Counter Technology-Facilitated Gender-Based Violence (2026–2030), outlining phased legal reforms, institutional strengthening, and targets to raise prosecution success rates from the current dismal levels (UNDP Pakistan, 2026).

Empirical data underscores systemic shortcomings. In the past five years, 1.8 million women in Pakistan have faced cybercrimes, yet only 3.5 percent of accused individuals have been convicted (WEBDESK, 2025). Over 8,000 cases were registered and 11,000 suspects arrested, but only 225, approximately 3.5 percent convictions were secured. In 2024 alone, approximately 160,000 complaints were logged, marking a decrease after years of rising numbers, partly due to amendments empowering police to register

cases, intending to tackle the growing digital crime problem (Devdiscourse News Desk, 2025). Civil society helplines, such as the Digital Rights Foundation's Cyber Harassment Helpline, recorded 3,171 new TFGBV cases in 2024, predominantly involving women (Digital Rights Foundation Pakistan, 2025), far exceeding formal registrations and highlighting massive underreporting and distrust in state institutions. Contributing factors to low conviction rates include police reticence, resource constraints, limited investigative capacity, jurisdictional overlap/ambiguity, evidentiary challenges in digital cases, cross-border platform issues, and inadequate gender-sensitive training. As the police now have discretionary power over the registration of cases, they are more inclined to settle disputes without formally registering a case.

Bangladesh

Bangladesh's Constitution provides foundational protections relevant to TFGBV. Article 27 guarantees equality before the law and equal protection of the law for all citizens, while Article 28 prohibits discrimination on grounds of sex. Article 39 secures freedom of thought and conscience, speech, and expression, subject to reasonable restrictions for public order, decency, morality, or defamation, and Article 43 provides protection of the home and correspondence. Although these provisions establish a constitutional basis for equality, privacy, and expressive freedoms, their application to digital contexts remains limited and often subordinated to broad state security and public morality concerns, resulting in uneven safeguards against online gendered harms.

The legislative framework has evolved rapidly. The Digital Security Act (2018) was replaced by the Cyber Security Act (2023), which was subsequently repealed by the interim government in 2024 and replaced with the Cyber Protection Ordinance (2024), also referred to as Cyber Security Ordinance or "Cyber Surokha Adhyadesh". In conjunction with the Pornography Control Act (2012), these instruments form the core of current responses to TFGBV. Relevant provisions criminalize privacy violations, online harassment, dissemination of obscene or defamatory content, and related offences.

Complementary provisions of the Penal Code (1860), notably Section 500 (defamation), and elements of the Pornography Control Act (2012) addressing coercive production and distribution of pornographic material, are frequently invoked in cases involving non-consensual intimate imagery, cyberstalking, and image-based abuse.

Despite these instruments, the framework is heavily critiqued as prioritizing state control instead of survivor-centered protections. The Cyber Protection Ordinance (2024) retains vague and overbroad provisions criminalizing content that may undermine "national unity", "public order", "religious values", as well as content deemed insulting or defamatory. Such provisions risk misuse against victims, journalists, activists, and minorities. Human rights organizations and legal experts argue that these laws emphasized government oversight and content regulation rather than recognizing misogynistic intent, consent violations, or the specific vulnerabilities of women, children, and marginalized groups in digital spaces. Emerging harms such as deepfakes and AI-generated abuse lack dedicated provisions, forcing reliance on general clauses ill-suited to address synthetic media.

Data protection remains fragmented and inadequate. Bangladesh lacks a comprehensive personal data protection law, though drafts of a Personal Data Protection Ordinance have circulated. In the absence of enacted legislation, survivors of doxxing, non-consensual image sharing, and deepfakes lack robust consent-based remedies or obligations on platforms and data processors. The overall administration continues to emphasize state security and morality-based restrictions over gender justice, with vague terminology facilitating selective enforcement, survivor-blaming, and chilling advocacy by women and human rights defenders.

Enforcement challenges further exacerbate legislative shortcomings. Police frequently dismiss TFGBV complaints as "non-serious" or family matters, compounded by evidentiary difficulties in digital cases, cross-border platform involvement, and limited technical capacity. Platform cooperation on content removal is inconsistent. Civil society

data highlighted the scale of problem: the Cyber Crime Awareness Foundation (2024) reported that cybercrime more than doubled in a single year, with nearly 60 percent of the victims being women. The Police Cyber Support for Women (PCSW) received over 9,000 harassment complaints in 2024 (Khalilullah, 2025). Surveys indicate that 63.51 percent of women have experienced online harassment, with broader violence against women studies revealing high lifetime exposure to various forms of abuse. Underreporting remains pervasive due to stigma, fear of retaliation, and distrust in institutions, resulting in widespread impunity. Deepfake and AI-facilitated abuse have surged, disproportionately targeting women, yet conviction rates remain low.

Sri Lanka

Sri Lanka's Constitution provides foundational protections relevant to TFGBV. Article 12 guarantees equality before the law and equal protection, while Article 14(1) protects freedom of speech and expression, subject to restrictions for public morality, public order, or the protection of rights of others. Article 13 and judicial interpretations support aspects of privacy, though a comprehensive, explicit right to privacy in digital contexts remains underdeveloped. In practice, the application of these rights to online gendered harms is inconsistent, with laws often prioritizing content control and public order over survivor-centered remedies and gender justice.

The core statutory framework includes the Computer Crimes Act (2007), which criminalizes unauthorized access to computers or data (Section 3), unauthorized modification or damage (Section 5), and related acts that can apply to doxing, hacking, or interference with private digital content. These provisions are supplemented by the Penal Code, addressing intimidation, harassment, and defamation (e.g., Section 500), and by the Pornography Control Act which regulates obscene or non-consensual material.

A landmark development is the Online Safety Act, No. 9 of 2024 (OSA), which came into force in February 2024. This Act establishes the Online Safety Commission with broad powers

to investigate and act on “prohibited statements” communicated online. Section 20 specifically addresses online harassment and the sharing of non-consensual private or personal information intended to harass, humiliate, or cause emotional distress. It also covers child protection, inauthentic accounts, and harmful content, with penalties including imprisonment and fines. Amendments in August 2024 and ongoing review processes in 2025/2026 have sought to refine intermediary liability and procedural safeguards, though scrutiny persists.

Critics, including human rights organizations and legal experts, argue that the OSA lacks explicit, gender-sensitive definitions for image-based sexual abuse, deepfakes, cyberstalking, or non-consensual intimate imagery as distinct TFGBV offences (Deckker & Sumanasekara, 2025). The vague provisions on “false statements,” “ill-will,” or threat to public order risk weaponization against victims, activists, journalists, and marginalized groups including LGBTQIA+ persons. The morality-oriented framing (focusing on decency and public order) rather than consent or misogynistic intent enables selective enforcement and survivor-blaming.

Sri Lanka enacted the Personal Data Protection Act (PDPA) (2022), South Asia's first comprehensive data law, phased in from 2023–2025 with amendments in 2025 refining timelines and rights. Although the PDPA provides general consent, security, and breach notification obligations, it is not tailored to TFGBV and lacks explicit integration with remedies for image-based abuse or gendered digital harms.

Statistics illustrate the scale of the problem: 5,400 cybercrime incidents were reported in the first six months of 2025 (Balasuriya, 2025). While constitutional guarantees and evolving laws, anchored by the Computer Crimes Act and the Online Safety Act, provide a nominal framework for TFGBV redress, the regime remains undermined by fragmented design, morality-oriented design, overbroad provisions prone to misuse, insufficient gender-sensitive provisions (particularly for deepfakes and image-based abuse), and chronic enforcement weaknesses. Ongoing amendments

to the OSA offer an opportunity for reform, but meaningful progress requires explicit redress mechanisms for consent-based offences, dedicated TFGBV provisions, stronger integration with the PDPA, mandatory gender-sensitive training for law enforcement, improved digital forensics capacity, and survivor-led monitoring mechanisms. Future scholarship and policy should prioritize empirical, disaggregated data and alignment with international standards to ensure digital spaces protect rather than endanger women and marginalized groups in Sri Lanka.

Where Did Legislation Fail?

In the context of TFGBV, legal frameworks systematically fail to adequately address gendered harms. This failure is often driven by patriarchal interpretations, victim-blaming attitudes, and narrow, tech-centric cybercrime approaches that obscure the structural nature of digital abuse. A socio-legal approach to TFGBV reveals a stark gap - progressive statutory protections may exist on paper, but they are routinely neutralized by enforcement biases or deeply entrenched cultural norms.

South Asia exemplifies a complex legal pluralism where formal state laws coexist with customary, religious, and informal dispute resolution systems (Menski, 2006). Informal systems such as *Shalish* proceedings in Bangladesh (Hoque, 2011), are highly accessible to local communities; however, they inherently reflect patriarchal biases that prioritize familial reconciliation over perpetrator accountability in GBV cases. Furthermore, broad police discretion plays a pivotal role in limiting legal efficacy (Barlow & Walklate, 2018). Law enforcement officials frequently divert TFGBV complaints to informal channels or exercise overt gender bias during intake (Sarkar et al., 2016). In South Asia, police officers often mediate family disputes informally, reinforcing victim-blaming tropes or pressuring survivors into extrajudicial settlements that severely undermine women's fundamental rights. This discretion, compounded by severe institutional resource constraints, widens the gap between formal ideal situations and lived realities,

underscoring the need for rigorous socio-legal scrutiny.

Enforcement Patterns and Central Critique

Across the region, law enforcement efforts reveal persistent structural barriers to addressing TFGBV. A primary challenge is the lack of a shared institutional understanding of TFGBV, which contributes to limited public awareness and weak institutional capacity within the justice system (The University of Melbourne & UNFPA Asia and the Pacific, 2024). Additional obstacles include systemic institutional reluctance, whereby TFGBV is routinely deprioritized in favor of financial crimes, volatility of digital evidence, limited forensic capacity, cross-border jurisdictional complexities, and inconsistent cooperation from international digital platforms regarding content removal and restricted data sharing (Neupane, 2026). Consequently, survivors experience re-traumatization, social stigma, and institutional distrust, which collectively drive significant underreporting.

The central critique of South Asian legal architectures is their over-reliance on punitive criminalization at the expense of survivor-centered justice. Existing legal frameworks primarily focus on punishing perpetrators while offering few restorative or remedial avenues, such as rapid image removal, trauma-informed support services, specialized courts, or accessible civil remedies (Bergman & et al., 2024). This punitive bias perpetuates a culture of impunity, effectively silences women's digital spaces, and fails to reconcile the competing constitutional rights of equality, privacy and freedom of expression. Comprehensive legal reform demands TFGBV-specific definitions, specialized gender-sensitive law enforcement units, corporate platform accountability, and holistic mechanisms that pivot toward substantive justice.

While countries like India, Bangladesh, and Pakistan have enacted cyber laws to supplement colonial-era or post-independence penal codes, these frameworks remain deeply flawed. They prioritize state-sanctioned punitive sanctions over survivor-centered mechanisms, exhibit a morality-

based rather than a right-based orientation, contain vague provisions prone to political misuse, and suffer from vast enforcement gaps. Although recent legislative modernization has been driven by an escalation in online harassment, image-based abuse, and emerging AI-generated harms such as deepfakes, persistent critiques highlight the danger of statutory overbreadth. These laws are frequently weaponized against women and political dissenters, fail to improve low conviction rates, and inadequately integrate constitutional guarantees of equality, privacy, and expression.

Socio- Cultural Barriers and the Limits of Legal Remedies

Socio-cultural barriers in South Asia constitute most entrenched obstacles undermining legal remedies to TFGBV. While formal legal frameworks exist across the region, their effectiveness is significantly weakened by entrenched socialized norms that prioritize family honor, social cohesion, and male hegemony over survivor-centric justice (Bergman & et al., 2024). These dynamics not only shape how digital violence is perceived but also determine whether survivors can safely access the justice system. As a result, digital harms are often privatized, normalized, or silenced.

Victim-blaming remains deeply embedded in societal responses to TFGBV across South Asia. Women are routinely held morally responsible for the abuse targeting them, with public narratives focusing on their online visibility and perceived deviation from moral norms (Generation G, n.d.). Female digital participation is often framed as inherently risky or inappropriate, reinforcing the patriarchal assumption that women who enter public online spaces “invite” harm (Perez et al., 2026). This framing shifts accountability away from perpetrators and discourages survivors from seeking formal legal remedies.

Furthermore, rigid “honor norms” intensify this barrier by tying women’s bodily and digital autonomy to familial and community reputation. Reporting TFGBV carries a prohibitive social cost, public exposure risks bringing institutionalized “shame” to the family (Equality Now, 2025).

Survivors often face intense domestic pressure to remain silent or withdraw complaints, leading to widespread underreporting. In some cases, the fear of reputational damage or escalation into offline violence, such as honor-based harm, compels families to suppress legal action entirely (Sambasivan & et al., 2019).

Informal justice systems, such as community councils and traditional mediation forums, play a prominent role in dispute resolution but consistently disadvantage women. These community-based mechanisms are frequently prioritized over state remedies because they emphasize social reconciliation. Reflecting localized patriarchal power structures, these mechanisms tend to trivialize digital harms and prioritize community harmony over individual accountability. Outcomes are often biased toward perpetrators, especially those possessing socio-economic or political influence. For marginalized women, intersections of caste, ethnicity, class, and gender further limit access to fair and equitable resolution. Family-mediated settlements, which pressure survivors to reconcile with abusers to avoid public scandal, commonly result in institutionalized revictimization.

The socio-cultural entrenchment of TFGBV also produces severe democratic repercussions, functioning as a silencing mechanism that excludes women from public discourse. Women in public-facing roles face highly disproportionate risks. In India, prominent journalist Rana Ayyub was targeted by coordinated deepfakes and doxxing campaigns designed to delegitimize her reporting (Ifraan, 2023). Similarly, in Pakistan, politician Azma Bokhari was targeted by a highly publicized deepfake scandal in 2024, prompting her temporary retreat from public life (France24, 2024). According to the Inter Parliamentary Union (2025) 60 percent of women Members of Parliament in the Asia Pacific region report experiencing TFGBV via doxxing and deepfakes. The data further indicates that specific demographics, particularly women under 40, women from minority backgrounds, and unmarried women, face disproportionately higher rates of violence (Inter Parliamentary Union, 2025).

As highlighted by the UN Secretary-General, anti-rights actors are increasingly using digital platforms to push back against women's rights, targeting women human rights defenders with cyberbullying, harassment, threats of violence, and gendered disinformation (UNGA, 2024). Approximately 73 percent of women journalists and public figures report being disproportionately targeted, with the rise of AI-generated deepfakes and synthetic imagery has intensifying the scale, velocity, and anonymity of these harms (UN Women, 2025).

Recent electoral and political crises illustrate this systemic suppression. During the March 2026 House of Representatives (HOR) elections in Nepal, female political candidates faced systematic, targeted TFGBV. A similar pattern emerged during Bangladesh's 2024 political uprising, where women's activities faced targeted and persistent TFGBV. The aggressive restriction of women's online visibility and political voice through TFGBV reinforces male dominance in governance, stifles dissent, discourages civic engagement, and erodes democratic pluralism. Addressing this crisis requires transformative structural reforms that challenge underlying patriarchal norms beyond purely statutory adjustments.

Survivors also encounter significant technical and institutional reporting barriers, including complex platform reporting interfaces, language accessibility limitations, social stigma, and non-responsive corporate moderation systems. Corporate transparency deficits compound these structural failures; multinational platforms rarely disclose detailed TFGBV-specific metrics or regional safety investments. Under the UN Guiding Principles on Business and Human Rights, technology companies bear a clear responsibility to conduct ongoing human rights due diligence to mitigate adverse impacts. However, deep tensions persist between corporate self-regulation and state intervention. While authoritarian states overreach risks weaponized censorship, insufficient corporate accountability allows digital harms to proliferate unchecked.

The escalation of digital disinformation campaigns targeting marginalized identities

further demonstrates the weaponization of these technologies. In India, the 2022 "Bulli Bai" application digitally "auctioned" prominent Muslim women, including outspoken journalists and pilots, in a mock exercise designed to degrade, humiliate, and silence those critical of rising ethno-nationalism (BBC, 2022). Although the perpetrators were subsequently arrested, the incident underscores how digital spaces are weaponized for gendered and sectarian terror. Nepal features similar trends; for instance, during a period of public protest against a political party leader, a female supporter was targeted with coordinated digital vitriol, including threats of rape and murder (BBC, 2022; Khabarhub, 2026).

Gender Divide: Unequal Access and Controlled Participation

While digital connectivity has undeniably expanded opportunities for women, enhancing access to information, mobilizing collective advocacy, and unlocking economic opportunity (UNFPA, 2024); the critical question remains whether these opportunities are equitably distributed.

In South Asia, the gender gap in mobile internet adoption in 2024 remained relatively high at 32 percent, leaving approximately 330 million women digitally disconnected (Jeffrie, 2022). Notably, of 885 million unconnected women globally, roughly 60 percent reside in South Asia and Sub-Saharan Africa (Jeffrie, 2022). Country-specific data reveals stark intra-regional disparities. While Pakistan's gender gap in mobile internet use narrowed to approximately 25 percent in 2024, (GSMA, 2025) 35 percent of female users rely on borrowed devices, severely compromising their digital privacy and autonomy (GSMA, 2025). Bangladesh had 26 percent female mobile internet use (Jeffrie, 2025a). Conversely, Nepal and Sri Lanka exhibit higher social media participation rates, with women comprising 44.3 percent (Kemp, 2025b) and 51.5 percent (Kemp, 2025a) of social media users, respectively.

Ultimately, the 2025 Global Gender Gap Report scores South Asia at 64.6 percent parity with its most severe and persistent barriers in economic participation and opportunity at 40.6 percent

(World Economic Forum, 2025). These metrics demonstrate that the core challenge is not merely a lack of infrastructural access, but rather a system of controlled and mediated access, wherein domestic and community power hierarchies dictate, police, and restrict women's digital autonomy.

Conclusion and way forward

Structural Continuity and Legal Fragmentations

The rapid expansion of digital technologies across South Asia has simultaneously created unprecedented opportunities for gendered expression and enabled the systemic expansion of TFGBV. This duality demonstrates that digital spaces are not distinct, autonomous environments, but are deeply embedded to sociopolitical realities. Rather than representing isolated, novel manifestation of abuse, TFGBV constitutes a digital amplification of pre-existing structural inequalities, patriarchal hegemonies, and institutionalized power imbalances that characterize the region.

While South Asian countries have increasingly adopted legal and regulatory frameworks to address online harms, these statutory responses remain largely fragmented, reactive, and grounded in morality-centric rather than rights-based paradigms. The systemic reliance on carceral criminalization as a primary legislative strategy has proven largely ineffective. Punitive measures fail to capture the highly nuanced, intersectional, and evolving nature of TFGBV, particularly as these harms are exacerbated by emerging generative artificial intelligence and synthetic media.

Fundamentally, existing legal architectures frequently lack conceptual clarity, specificity, and survivor-centered remedies, resulting in gaps between formal protections and the lived experiences of survivors. These enforcement gaps are compounded by socio-cultural barriers, including deeply socialized victim-blaming and rigid honor norms, alongside a persistent gender digital divide that limits women's technical autonomy and normalizes digital violence. Beyond individual harm, TFGBV also undermines democratic participation by silencing women in public life.

Democratic Repercussion and Corporate Accountability

Beyond individual psychological and physical precarity, TFGBV poses severe, systemic risks to democratic governance. By systematically targeting and silencing women in public-facing roles, particularly journalists, human rights activists, and political actors, TFGBV deliberately distorts public discourse, erodes inclusive participation, and reinforces traditional hierarchies of power. The institutionalized normalization of this digital violence not only limits fundamental freedoms but actively compromises the democratic pluralism and governance architectures of South Asian nations.

Therefore, confronting TFGBV requires an immediate paradigm shift away from narrow, punitive approaches toward holistic, rights-based, and survivor-centered legal frameworks. Comprehensive reform demands the codification of explicit statutory definitions for TFGBV, integration of affirmative, consent-based legal standards, strengthening of robust data privacy systems, and establishment of accessible civil remedies to complement criminal sanctions. Parallel institutional re-engineering is equally critical; this includes the implementation of mandatory, gender-sensitive judicial training, the improvement of localized digital forensic capacities, and the establishment of specialized adjudicative mechanisms to ensure timely redress.

However, formal legal interventions are insufficient without a calculated response to the socio-cultural foundations of gender inequality. A critical intervention lies in expanding critical digital literacy, fostering community-led counter narratives, and dismantling the honor-shame binaries that perpetuate silence and stigma. Concurrently, international technology conglomerates must be held strictly accountable through stringent regulatory frameworks that mandate corporate transparency, localized content moderation responsiveness, and strict compliance with international human rights standards.

Ultimately, the challenge of TFGBV in South Asia is neither an architectural glitch of

technology nor a simple gap in statutory drafting; it is an issue of deeply structural violence. As South Asia accelerates its digital transition, the failure to redress these underlying inequalities risks entrenching new, highly durable vectors of digital exclusion and harm. Conversely, an integrated, multi-sectoral strategy that bridges legal reform, corporate accountability, and structural social transformation offers an opportunity to reclaim digital architectures as sites of safety, equality, and democratic spaces for all.

References

- ABC7 Chicago. (2012, July 17). *Yahoo CEO's pregnancy reignites a perennial debate*. ABC7 EyeWitness News. <https://abc7chicago.com/archive/8739851/>
- Agyare, P. (2025). Gendered digital arms and youth ideological trajectories: Socioeconomic challenges of digital platforms. *SocioEconomic Challenges*, 9(3), (P. 83) https://www.researchgate.net/publication/396500204_Gendered_Digital_Harms_and_Youth_Ideological_Trajectories_Socioeconomic_Challenges_of_Digital_Platforms
- Amnesty International. (2017, November 20). *Amnesty reveals the alarming impact of online abuse against women*. [Press release]. <https://www.amnesty.org/en/latest/press-release/2017/11/amnesty-reveals-alarming-impact-of-online-abuse-against-women/>
- Amnesty International. (2025, January 24). *Pakistan: Authorities pass bill with sweeping controls on social media*. <https://www.amnesty.org/en/latest/news/2025/01/pakistan-authorities-pass-bill-with-sweeping-controls-on-social-media/>
- Balasuriya, D. S. (2025, July 25). Over 5,400 cybercrime cases in 2025; CID warns of job, investment scams Cybercrime rises in Sri Lanka. *Daily Mirror*. <https://www.dailymirror.lk/front-page/Over-54-000-cybercrime-cases-in-2025-CID-warns-of-job-investment-scams-Cybercrime-rises-in-Sri-Lanka/238-315197>
- Barlow, C., & Walklate, S. (2018). Policing intimate partner violence: The “golden thread” of discretion. *Policing: A Journal of Policy and Practice*, 14(2). <https://doi.org/10.1093/police/pay001>
- BBC News. (2022, January 10). Sulli Deals: Police arrest man for making app to auction Muslim women. <https://www.bbc.com/news/world-asia-india-59933029>
- Bergman, S., & et al. (2024). *Understanding technology-facilitated gender-based violence in Asia - A qualitative study*. UNFPA Asia and the Pacific. https://asiapacific.unfpa.org/sites/default/files/pub-pdf/202410/Understanding%20technology-facilitated%20gender-based%20violence%20in%20Asia_1.pdf
- Bergman, S., & et al. (2024). *Understanding technology-facilitated gender-based violence in Asia - A qualitative study*. UNFPA Asia and the Pacific. https://asiapacific.unfpa.org/sites/default/files/pub-pdf/202410/Understanding%20technology-facilitated%20gender-based%20violence%20in%20Asia_1.pdf
- Bhatt & Joshi Associates. (2026, April 15). *The Jurisprudence of synthetic reality: A comprehensive legal and constitutional analysis of India's IT Amendment Rules 2026*. <https://bhattandjoshiassociates.com/the-jurisprudence-of-synthetic-reality-a-comprehensive-legal-and-constitutional-analysis-of-indias-it-amendment-rules-2026/>
- Chand, A. (2026, February 1). Women election candidates in Nepal face abuse and vitriol. *The Kathmandu Post*. <https://kathmandupost.com/politics/2026/02/01/women-election-candidates-in-nepal-face-abuse-and-vitriol>
- Children Act, 66 (3) (2018). <https://goodweavecertification.org.np/Resources/assets/files/childrenAct2075English.pdf>
- Computer Crime Act, No. 24 of 2007 (Sri Lanka). <https://www.srilankalaw.lk/revised-statutes/volume-ii/239-computer-crime-act.html>
- Cyber Security Act, 2023 (Bangladesh).

- Devdiscourse News Desk. (2025, January 15). *Pakistan's struggle with cybercrime: Low conviction rates and evolving strategies*. Devdiscourse. <https://www.devdiscourse.com/article/international/3225912-pakistans-struggle-with-cybercrime-low-conviction-rates-and-evolving-strategies>
- Digital Rights Foundation Pakistan. (2025, April 24). *Over 20,000 cases of Technology-Facilitated Gender-Based Violence (TFGBV) received by Digital Rights Foundation's Helpline during 8 years of operation*. <https://digitalrightsfoundation.pk/subject-over-20000-cases-of-technology-facilitated-gender-based-violence-tfgbv-received-by-digital-rights-foundations-helpline-during-8-years-of-operation/>
- Digital Security Act, 2018 (Bangladesh). <https://www.basis.org.bd/public/files/policy/5e1653db166e8Digital-Security-Act-2018-English-version.pdf>
- Deckker, D., & Sumanasekara, S. (2025). Digital Gender Violence in Sri Lanka: A review of emerging trends, legal frameworks and policy gaps. *World Journal of Advanced Research and Reviews*, 27(3), 1937. <https://doi.org/10.30574/wjarr.2025.27.3.3367>
- Electronic Transaction Act, 2006 (Nepal). <https://lawcommission.gov.np/content/13397/electronic--electronic--traded-international-act--2063/>
- Equality Now. (2025, November 1) *Experiencing technology-facilitated gender-based violence in India*. <https://equalitynow.org/resource/reports/experiencing-technology-facilitated-gender-based-violence-in-india/> Experiencing technology-facilitated gender-based violence in India - Equality Now
- France24. (2024, March 10). *Deepfakes weaponised to target Pakistan's women leaders*. <https://www.france24.com/en/live-news/20241203-deepfakes-weaponised-to-target-pakistan-s-women-leaders>
- Francis, A. M. (2025, October 23). Online Crimes Against Women in India: Deepfakes, Doxxing, and Digital Abuse - Centre for Public Policy Research (CPPR). Centre for Public Policy Research (CPPR). <https://www.cppr.in/articles/deepfakes-doxxing-and-digital-abuse>
- Generation G. (n.d.). *Decoding Technology-Facilitated Gender-Based Violence*. Rutgers International. <https://rutgers.international/wp-content/uploads/2024/06/Decoding-TFGBV-Report-2024.pdf>
- GSMA. (2025). *A breakthrough year for women's Digital Inclusion in Pakistan*. <https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/wp-content/uploads/2025/06/A-Breakthrough-Year-for-Womens-Digital-Inclusion-in-Pakistan-.pdf>
- Hoque R., Judicial activism in Bangladesh: A golden mean approach. University Press Limited. <https://scispace.com/pdf/judicial-activism-in-bangladesh-a-golden-mean-approach-3d8imsj552.pdf>
- Ifran, A. (2023, June 5). *Gender, AI and the psychology of disinformation*. Media Diversity Institute. <https://www.media-diversity.org/gender-ai-and-the-psychology-of-disinformation/>
- Indian Penal Code, 1860 (India). <https://www.indiacode.nic.in/bitstream/123456789/4219/1/THE-INDIAN-PENAL-CODE-1860.pdf>
- Individual Privacy Act, 2018 (Nepal). <https://lawcommission.gov.np/content/12261/12261-the-privacy-act-2075/>
- Information Technology Act, 2000 (India). https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf
- Information Technology and Cyber Security Bill, 2025 (Nepal). <https://hr.parliament.gov.np/en/bills/njBRB4qb>
- Inter Parliamentary Union. (2025, March 25). *60% of women MPs from Asia-Pacific report online gender-based violence* [Press release]. <https://www.ipu.org/news/>

- press-releases/2025-03/60-women-mps-asia-pacific-report-online-gender-based-violence
- Inter Parliamentary Union. (n.d.). *Sexism, harassment and violence against women in parliaments in the Asia-Pacific region* [Issue Brief]. <https://www.ipu.org/resources/publications/issue-briefs/2025-03/sexism-harassment-and-violence-against-women-in-parliaments-in-asia-pacific-region>
- Iyer, N., Nyamwire, B., & Nebulega, S. (2020, August 4). *Alternate realities, alternate internets: African feminist research for a feminist internet* | Association for Progressive Communications. Policy. <https://www.apc.org/en/pubs/alternate-realities-alternate-internets-african-feminist-research-feminist-internet>
- Jeffrie, N. (2022). *The mobile gender gap report 2025*. GSMA.
- Jeffrie, N. (2025a). *The mobile gender gap report 2025*. GSMA. https://www.gsma.com/wp-content/uploads/2025/12/The-Mobile-Gender-Gap-Report-2025.pdf?utm_source=website&utm_medium=button&utm_campaign=gender-gap-2025
- Justice K.S. Puttaswamy (Retd) vs Union Of India, Writ Petition (Civil) No. 494 of 2012 (Supreme Court of India September 26, 2018). <https://indiankanoon.org/doc/127517806/>
- Kate. (2021, September 29). *I'm a new mother – and that's evidently a big problem for some Big Tech companies*. ACLU Illinois. <https://www.aclu-il.org/news/im-new-mother-and-thats-evidently-big-problem-some-big-tech-companies/>
- Kemp, S. (2025a, March 3). *Digital 2025: Sri Lanka*. DataReportal. <https://datareportal.com/reports/digital-2025-sri-lanka>
- Kemp, S. (2025b, March 3). *Digital 2025: Nepal*. DataReportal. <https://datareportal.com/reports/digital-2025-nepal>
- Kemp, S. (2025a, November 5). *Digital 2026: India*. DataReportal. <https://datareportal.com/reports/digital-2026-india>
- Kemp, S. (2025b, November 8). *Digital 2026: Pakistan*. Data Reportal. <https://datareportal.com/reports/digital-2026-pakistan>
- Kemp, S. (2025c, November 8). *Digital 2026: Sri Lanka*. Data Reportal. <https://datareportal.com/reports/digital-2026-sri-lanka>
- Kemp, S. (2025d, November 8). *Digital 2026: Bangladesh*. Data Reportal. <https://datareportal.com/reports/digital-2026-bangladesh>
- Kemp, S. (2025e, November 8). *Digital 2026: Nepal*. Data Reportal. <https://datareportal.com/reports/digital-2026-nepal>
- Khabarhub. (2026). *Complaint filed after cyber harassment targeting woman supporting KP Oli*. <https://english.khabarhub.com/2026/01/542090/>
- Khalilullah, I. (2025, May 29). *Cyber violence is silencing women in Bangladesh*. South Asia Monitor. <https://www.southasiamonitor.org/index.php/spotlight/cyber-violence-silencing-women-bangladesh>
- Khan, Dr. I. A., Irshad, S., & Ud Din , H. S. J. (2025). Cyber harassment and online violence against women :A critical analysis of women protection law regime in Pakistan. *Journal of Law & Social Studies*, 7(1), 12–25. <https://doi.org/10.52279/jlss.07.01.1225>
- MacKinnon, C.A. (1989) *Toward a Feminist Theory of the State*. Harvard University Press.
- Menski W., *Comparative law in a global context: The legal systems of Asia and Africa* (2nd ed.). Cambridge University Press. Cited in Islam F. Legal pluralism in South Asia: The sustainable Role of customary law in modern legal systems. *Journal of Legal research and Policy*, 2(2):67-88. Available from: <https://jlrp.in/index.php/jlrp/article/view/41>
- National Penal Code, 2017 (Nepal). <https://lawcommission.gov.np/content/13454/criminal-code-2074/>
- National Statistics Office. (2025). *National accounts*

- statistics of Nepal 2024/25 national report*. Government of Nepal, Office of the Prime Minister and Council of Ministers. https://giwmscdnone.gov.np/media/pdf_upload/National%20Report_bzpm6lk.pdf
- Nepal Police. (2023). *Annual Fact Sheet on Suicide and Cyber Crime*. (n.d.). https://www.nepalpolice.gov.np/media/filer_public/55/b3/55b3b954-7fee-40fc-b661-7db2d9604574/fy-2081-82-suicide-cyber-crime-ne-1.pdf
- Nepal Police. (2023). *Police Mirror 2025*. https://www.nepalpolice.gov.np/media/filer_public/36/6a/366a793e-ebe4-4e82-b0bc-74486313950b/1_nepal_police_mirror_2025.pdf
- Neupane, R. (2026). The perils of fragile institutions. *The Kathmandu Post*. <https://kathmandupost.com/columns/2023/11/07/the-perils-of-fragile-institutions>
- Pakistan Penal Code, 1858 (Pakistan). <https://www.pakistani.org/pakistan/legislation/1860/actXLVof1860.html>
- Perez, A. P., Farrell, T., Kock, C. D., Jurasz, O., Nozza, D., & Fernandez, M. (2026, April). *Still unsafe: what's holding us back on online safety for women*. ResearchGate. https://www.researchgate.net/publication/403693428_Still_unsafe_what's_holding_us_back_on_online_safety_for_women
- Personal Data Protection Act, No 9 of 2022 (Sri Lanka). <https://www.parliament.lk/uploads/acts/gbills/english/6242.pdf>
- Pornography Control Act, 2012 (Bangladesh) <http://bdlaws.minlaw.gov.bd/act-details-1091.html>
- Prevention of Electronic Crimes Act, 2016 (Pakistan). https://www.na.gov.pk/uploads/documents/1470910659_707.pdf
- Privacy International. (2023, August 8). *Privacy International raises concerns regarding Pakistan's Personal Data Protection Bill*. <https://privacyinternational.org/news-analysis/5090/privacy-international-raises-concerns-regarding-pakistans-personal-data>
- Renström, E. A., & Bäck, H. (2024). Manfluencers and young men's misogynistic attitudes: the role of perceived threats to men's status. *Sex Roles*, 90(12). <https://link.springer.com/article/10.1007/s11199-024-01538-2>
- Sambasivan, N., & et al. (2019). *"They don't leave us alone anywhere we go": Gender and digital abuse in South Asia*. Google Research. <https://research.google/pubs/they-dont-leave-us-alone-anywhere-we-go-gender-and-digital-abuse-in-south-asia/>
- Sarkar, A., Mukhopadhyay, D., Blake, C., & Prasad, D. (2016, June 24). *Crime victimization and safety perception: A public survey of Delhi and Mumbai*. Research Gate. https://www.researchgate.net/publication/312146858_Crime_victimization_and_safety_perception_A_public_survey_of_Delhi_and_Mumbai
- Scasserra, N. B. (2024, October 3). *Digital Capitalism | Transnational Institute*. Transnational Institute. <https://www.tni.org/en/publication/digital-capitalism>
- Shinde, S. (2026, March 15). Deepfake attacks rise 900%, most women take "no action": Report. Business Standard. https://www.business-standard.com/technology/tech-news/deepfake-attacks-rise-900-most-women-take-no-action-report-126031500844_1.html
- Singh, S. D., & Ferraz, J. (2023, October 20). *Digital transformation and inclusivity: Reshaping Asia and the Pacific's urban future*. United Nations ESCAP. <https://www.unescap.org/blog/digital-transformation-and-inclusivity-reshaping-asia-and-pacifics-urban-future>
- Storyboard18. (2026, March 19). *Cybercrime against women rises sharply in 2025, crosses 76,000 cases: Govt*. News18. <https://www.storyboard18.com/digital/cybercrime-against-women-rises-sharply-in-2025-crosses-76000-cases-govt-ws-e-92736.htm>
- SVRI, The Global Partnership, APC, & UN Women. (n.d.). *Technology facilitated gender-based violence: Developing a shared research agenda*. <https://unwomen.org>

- org/sites/default/files/2024-09/technology-facilitated-gender-based-violence-shared-research-agenda-en.pdf
- The Annapurna Express. (2025, November 23). *Reclaiming feminism in South Asia* <https://theannapurnaexpress.com/story/60182/>
- The Bharatiya Nyaya Sanhita, 2023 (India). <https://www.indiacode.nic.in/bitstream/123456789/20062/1/a202345.pdf>
- The Digital Personal Data Protection Act, 2022 (India). <https://www.indiacode.nic.in/bitstream/123456789/22037/1/a2023-22.pdf>
- The Penal Code, 1860 (Bangladesh) <http://bdlaws.minlaw.gov.bd/act-11.html>
- The University of Melbourne & UNFPA Asia and the Pacific. (2024, October 14). *Understanding technology-facilitated gender-based violence in Asia: A qualitative study*. UNFPA Asia-Pacific. <https://asiapacific.unfpa.org/en/publications/understanding-technology-facilitated-gender-based-violence-asia-qualitative-study>
- Transnational International. (2024). *Digital Capitalism*. <https://www.tni.org/en/publication/digital-capitalism>
- UN Women, & World Health Organization. (2022). *Technology-facilitated violence against women: Towards a common definition*. <https://www.unwomen.org/sites/default/files/2023-03/Expert-Group-Meeting-report-Technology-facilitated-violence-against-women-en.pdf>
- UN Women. (2021). *Violence against women in the online space: insights from a multi-country study in the Arab States*. UN Women Arab States. <https://arabstates.unwomen.org/en/digital-library/publications/2021/11/violence-against-women-in-the-online-space>
- UN Women. (2024). *The dark side of digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia*. UN Women Europe and Central Asia. <https://eca.unwomen.org/en/digital-library/publications/2023/11/the-dark-side-of-digitalization-technology-facilitated-violence-against-women-in-eastern-europe-and-central-asia>
- UN Women. (2025, February 10). *FAQs: Digital abuse, trolling, stalking, and other forms of technology-facilitated violence against women*. <https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women>
- UNFPA. (2024, November 28). *Digital duality: How the internet empowers and endangers women*. <https://caribbean.unfpa.org/en/news/digital-duality-how-internet-empowers-and-endangers-women>
- UNFPA. (n.d.). *Technology-facilitated gender-based violence: a growing threat*. <https://www.unfpa.org/TFGBV>
- UNGA, (2024) *Intensification of efforts to eliminate all forms of violence against women and girls: technology-facilitated violence against women and girls*, Report of the Secretary General (A/79/500). <https://docs.un.org/en/A/79/500>
- UNDP Pakistan. (2026, March 10). *Ministry of Human Rights and UNDP launch Pakistan's first National Strategy on Technology-Facilitated Gender-Based Violence*. <https://www.undp.org/pakistan/press-releases/ministry-human-rights-and-undp-launch-pakistans-first-national-strategy-technology-facilitated-gender-based-violence>
- WEBDESK. (2025, March 16). *Pakistan: 1.8 million women targeted by cybercrimes in 5 years, conviction rate at just 3.5 percent*. Organiser. <https://organiser.org/2025/03/16/282360/world/pakistan-1-8-million-women-targeted-by-cybercrimes-in-5-years-conviction-rate-at-just-3-5-percent/>
- World Economic Forum. (2025). *Global gender gap report 2025*. https://reports.weforum.org/docs/WEF_GGGR_2025.pdf

