IN BRIEF

MODEL FRAMEWORK FOR LEGISLATION ON TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN AND GIRLS

Overview

Technology-facilitated violence against women and girls (TF VAWG) is a growing and pervasive concern that affects women and girls across all regions and countries of the world. Although the patterns and the forms of TF VAWG can be unique, they occur as part of a continuum of multiple, recurring and interrelated forms of violence against women and girls, which are often connected to violence offline. In recent years, thanks to feminist mobilization and advocacy , international and regional frameworks have increasingly recognized the need for legislation on TF VAWG. Major gaps, however, still persist in legal protections, with more than half the global population of women still unprotected.[1] Fewer than 40 per cent of countries worldwide provide legal protections against cyberharassment, 93 per cent of which provide criminal penalties, and only 14 per cent offer civil remedies.[2] Even where legislation does exist, laws do not usually include the full spectrum of TF VAWG and have failed to keep pace with rapid technological change.

As outlined in the UN Secretary-General's latest report on VAWG, some forms of TF VAWG are an extension of existing forms of VAWG – e.g. sexual harassment, intimate partner violence, stalking, trafficking – which in some jurisdictions could be covered by existing VAWG legislation as the same protections should apply whether the crime occurred in a digital space or a physical space. Meanwhile, for other more novel forms of TF VAWG – such as the creation and dissemination of non-consensual intimate images or deepfake videos – existing laws might not provide adequate protection.[3] Comprehensive laws addressing the full spectrum of TF VAWG is imperative to end impunity and ensure justice, protection and support for victims/survivors.

Purpose of this brief

This brief presents the main elements of the forthcoming *Supplement to the Handbook for Legislation on Violence against Women on Technology-Facilitated Violence against Women and Girls*. It is meant to be read in conjunction with the Handbook for Legislation on Violence against Women, which provides detailed guidance to support the adoption and effective implementation of legislation that prevents violence against women, punishes perpetrators and ensures the rights of victims/survivors everywhere. The supplement aims to guide legislators in the adoption or the revision of laws to ensure legal frameworks provide the necessary protection and remedies to prevent and respond to TF VAWG, by setting clear recommendations on what legislation should be addressing to meet global norms and standards and reflect the latest lessons learned from country experiences across all world regions.[4] These recommendations are underpinned by shared principles and standards that can be adapted and localized across different countries and jurisdictions in the world.

This brief was prepared by the Ending violence against Women and Girls Section of UN Women, based on research and expert consultations across all five world regions led by the Association of Progressive Communications (APC) in 2024 and 2025. APC is an international network of civil society organizations dedicated to empowering and supporting people working for peace, human rights, development and environmental protection through the strategic use of information and communications technologies. The brief was reviewed by Catherine Van De Heyning, Expert Rapporteur on TF VAWG for the UN Human Rights Council (HRC) Advisory Committee, Professor of fundamental rights law at the University of Antwerp and Deputy Public Prosecutor in Antwerp's cybercrime division. She was recognized as the 2025 Cyber Security Personality of the Year by the Belgian Cyber Security Coalition for her advocacy.

Defining TF VAWG

There is currently no internationally agreed terminology or definition of technology-facilitated violence against women. Technology-facilitated violence against women and girls is also known interchangeably as "information and communications technology-facilitated violence", "online violence", "tech-facilitated or related violence", "digital violence" or "cyberviolence." The Resolution on the Intensification Global Digital Compact and the Agreed Conclusions of the sixty-seventh session of CSW on innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls refer to forms of violence that 'occur through or are amplified by the use of technology.'[5] In the present brief, the term "technology-facilitated violence against women and girls" has been utilized to align with the language recently used by the Statistical Commission at its fifty-fifth session as well as with the working definition that was proposed at a UN Women-convened Expert Group Meeting in 2022.[6]

Defining technology-facilitated violence against women and girls

TF VAWG is any act that is committed, assisted, aggravated or amplified by the use of information communication technologies or other digital tools which results in or is likely to result in physical, sexual, psychological, social, political or economic harm or other infringements of rights and freedoms. These are forms of violence that are directed against women because they are women and/or that affect women disproportionately.

Global and regional legal and policy frameworks on TF VAWG legislation

The obligation of States to enact legislation to address VAWG has been established in international human rights treaties,[7] with recent clarifications that legislation should apply to TF VAWG[8] on the core principle that "the same rights that people have offline must also be protected online."[9]

National legislation on TF VAWG must be anchored in international law, including international human rights law. Over the past decade, global and regional frameworks have moved from implicit recognition of TF VAWG to more direct articulation.[10] This principle was reaffirmed in the Global Digital Compact,[11] while the General Assembly resolution 79/152 on the intensification of efforts to eliminate all forms of violence against women and girls: the digital environment (2024)[12] urges Member States to take measures to prevent and protect women from violence online and through digital technologies, and to adopt laws and policies to protect them from defamation and hate speech. Additional forms of TF VAWG are particularly identified in global instruments as specific threats to women's human rights, such as hate speech, defamation, misinformation, disinformation, cyberbullying and child sexual exploitation and abuse.

The Convention against Cybercrime requires the adoption of legislation criminalizing the non-consensual dissemination of intimate images and online child sexual abuse or exploitation.[13]

Global frameworks also identify the special application of international human rights law with regards to aspects related to TF VAWG, including by calling for the creation of oversight and remedy mechanisms; by refraining from imposing restrictions on the free flow of information and ideas; through due diligence for surveillance and encryption laws and regulations; and via data protection or the governance of artificial intelligence and digital public goods.

Regional frameworks have likewise evolved in the past five years, providing an increasingly targeted framework on legislation related to digital developments and TF VAWG.[14]

The European Union's Directive 2024/1385 on combating violence against women and domestic violence[15] establishes criminal law, victim-support, procedural and enforcement obligations on cyber-violence against women.

Addressing gaps, challenges and tensions in legal frameworks on TF VAWG

One of the key challenges in developing laws addressing TF VAWG is the lack of a universally agreed definition and standardized terminology which would be foundational for consistent legislation and protection globally.[16] Given the borderless nature of cyberspace and digital platforms,

transnational cooperation is required to effectively address TF VAWG and this makes a common language and framework of protection paramount.[17]

Furthermore, the fast-paced nature of technological developments has made it difficult for laws to keep pace with the emerging forms of technology-facilitated VAWG and the scale of harm introduced by digital tools and AI. Laws criminalizing certain forms of TF VAWG raise tensions at the intersection of the rights of digital users to freedom of expression, access to information, privacy, personal autonomy and a life free from violence. It is therefore essential to ensure that legislation does not contain provisions that can be weaponized against women and girls – particularly those already at heightened risk, such as women in public life or from marginalized groups.[18] For example, overly broad laws may be misused to silence civil society voices or human rights defenders or anyone criticizing the authorities by removing legitimate online content, thereby infringing upon freedom of expression.[19]

At the same time, when considering freedom of expression, it is important to note the silencing effect of TF VAWG and to recognize the need for legal limitations on abusive expression to ensure women in all their diversity can participate safely in digital spaces.[20] As the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression argues, there can be no trade-off between women's right to be free from violence and the right to freedom of opinion and expression. Both rights must be equally upheld by States.[21] Yet, striking the right balance between the protection of free speech and the need to ensure freedom from violence and discrimination continues to be a challenge. Independent or judicial oversight is key to ensuring that laws to prevent TF VAWG are proportionate and not used to silence legitimate expression while still upholding the right of women and girls to live free from violence.

It is also important to note the potential for unintended harms for women and girls of some legislation. For instance, laws designed to prevent the non-consensual sharing of intimate images can, in some cases, inadvertently criminalize women or adolescents who have taken or shared intimate images of themselves. In some States, tech/social media platforms may be required to proactively monitor or put in place automated content moderation to take down harmful content that may inadvertently incentivize over-removal and the takedown of newsworthy/legitimate content by platforms. Moreover, this can also serve to restrict expression and serve to criminalize the very people that such measures should protect, such as women human rights defenders.[22]

Some governments and regulators argue for weakening end-to-end encryption to help detect criminal activity, address child sexual abuse material, or enable faster access to evidence for law enforcement. However, weakening encryption can increase gendered harms. For many victims/survivors of domestic violence, sexual violence, stalking and trafficking, strong encryption is key to ensuring they have private and secure ways to contact support services, coordinate escape plans, or document their experiences to preserve evidence for legal action. Encryption can also ensure that perpetrators cannot access victims/survivors' communication and information.[23]

As with other forms of VAWG, a significant challenge is that victim/survivors often do not report TF VAWG due to the normalization of violence, and social norms. Research shows that TF VAWG is widely normalized, minimized or dismissed by law enforcement and technology companies.[24] A lack of awareness that TF VAWG is criminalized coupled with fear, lack of trust or confidence or information about where or to whom they should report is also a roadblock.[25] Finally, limited capacities of law enforcement to adapt to rapid technological advancement and the global, borderless nature of cyberspace, means that online crimes often occur outside the jurisdiction of law enforcement agencies. Such challenges contribute to a climate of impunity even where legislation does exist. Legal systems and law enforcement in many jurisdictions have not yet caught up and may therefore ignore or not take TF VAWG reports as seriously.[26] This is further exacerbated by systemic gender bias, discriminatory norms and stereotypes within the law enforcement sector which are also barriers to effectively enforce legislation. Addressing gender bias and sexist stereotypes within the law enforcement sector is critical to ensuring an effective or fair legal response for all victims-survivors of TF VAWG.[27]

Guiding principles for legislation on TF VAWG

As digital platforms become increasingly central to public discourse, political participation, education, work, and activism, the online sphere mirrors and often magnifies existing power imbalances and systemic inequalities.

Effective legislation on TF VAWG must be grounded in a rights-based, victim/survivor-centered framework that protects the dignity of those most impacted by TF VAWG, does not revictimize victims/survivors, confronts structural drivers of digital violence and ensures a proportional balance between different rights such as freedom of expression and privacy, and the right to freedom from discrimination and violence. Legislation should be evidenced-based and designed through participatory approaches. Potential impact of the legislation should be carefully assessed, ensuring meaningful participation of women and girls in all their diversity, particularly those groups most affected such as women in public life, including women human rights defenders, activists, journalists and politicians and women who experience multiple, intersecting forms of discrimination.

1

Guiding principle 1: Intersectionality

A 'one-size-fits-all' approach to addressing TF VAWG risks ignoring how some groups such as young women, women with migrant backgrounds or in migration, women from religious or ethnic minorities, including Black and Indigenous women, lesbian, gay, bisexual, transgender, queer, intersex and other (LGBTQI+) persons, women with disabilities and women in public life face heightened risks of TF VAWG, compounded harms and systemic barriers when accessing justice. Legislation should adopt an intersectional lens and address the lived realities and the diverse needs of those most affected by TF VAWG to ensure that it does not lead to harmful or misaligned interventions.

2

Guiding principle 2: Autonomy and agency – empowering survivors

The principle of autonomy and agency affirms the right of individuals – especially those who are marginalized or criminalized – to make informed decisions about their bodies, identities, data and participation in public and private life. It is critical for any legal framework on TF VAWG to recognize and restore the autonomy of survivors by avoiding to surveil or silence those they claim to protect. Legislators should avoid paternalistic or protectionist approaches that override survivor choices, and aim to uphold the right to digital self-determination, including control over online presence, consent to data usage and digital disengagement, when desired. At the same time, it is important to take a life course approach, recognizing that TF VAWG manifests differently across life stages and that there are differing legal and normative obligations towards women, adolescents and children. Child protection responses grounded in international child rights frameworks recognize children's evolving capacities, their dependent status and responsibilities of caregivers and authorities to act in their best interests.[28] These principles are essential for protecting children but they are not designed for women. Adolescent girls are a group that often slip through the cracks and may be overlooked by both child protection and EVAW policy/programming. For adolescent girls it is important to apply survivor-centred principles in ways that respect adolescents' evolving capacities, agency and rights under international child rights law.[29]

3

Guiding principle 3: Consent

Consent is a foundational concept in addressing TF VAWG, particularly in contexts such as image-based abuse, data collection and online interactions. Consent must be understood as freely given, informed, specific and revocable and not presumed, coerced or extracted under duress. Legislation should move away from intent-based approaches and promote consent as a central element, or risk being insufficiently effective. This includes the clear prohibition of non-consensual acts and incorporating affirmative consent standards in defining violations and liabilities.

4

Guiding principle 4: Transparency and accountability

The principle of transparency and accountability ensures that laws, enforcement practices, platform policies and technological systems are subject to public scrutiny and democratic oversight. TF VAWG often thrives in opaque environments, whether through algorithmic bias, secretive surveillance or unaccountable content moderation by private platforms. This principle applies to both public and private actors, notably through the creation of accountability mechanisms for State and non-State actors, mandating public reporting on TF VAWG case-handling, legal outcomes and system gaps, and requiring transparency from platforms about their moderation.

Model framework for legislation on technology-facilitated violence against women and girls: an overview of main recommendations

The recommendations below present the core elements of the model legislative framework on TF VAWG, which will be fully elaborated in the forthcoming *Supplement on TF VAWG* to the *Handbook for Legislation on Violence against Women*.

1. Human rights-based and comprehensive approach

TF VAWG as a form of gender-based discrimination

TF VAWG legislation should explicitly recognize TF VAWG as a form of gender-based discrimination and a violation of women's human rights.

Legislation on TF VAWG should:

- Acknowledge the diverse manifestations of harm created by TF VAWG, both online and offline
- Respond to the needs of those most at risk or affected
- Ensure that protection mechanisms are accessible and inclusive
- Not reinforce existing exclusions or inequalities.

Comprehensive legislative approach

As with any legislation on VAWG, the legislative approach to TF VAWG should be comprehensive, addressing the full spectrum of violence – from its root causes to its profound impacts – rather than focusing solely on responding to individual incidents. Criminalization should be complemented with civil remedies and administrative law provisions to offer diverse options to victims/survivors. Criminal provisions must be closely weighed to ensure they are not used to punish consensual sexual expression or silence dissent, with a risk of expanding surveillance or restricting expression in the name of protection. All restrictions of freedom of expression must comply fully with the three-part test of legality, necessity and proportionality, and legitimate objectives, as set out in the International Covenant on Civil and Political Rights.

Legislation on TF VAWG should:

- Criminalize all forms of TF VAWG
- Enable effective prosecution and appropriate penalties for perpetrators
- Mandate strategic prevention measures from public institutions and tech platforms
- Guarantee survivor empowerment, support and protection.

In 2023, Argentina enacted its own 'Olimpia Law',[30] inspired by the original Olimpia Law in Mexico,[31] amending the *Integral Protection Law to Prevent, Punish and Eradicate Violence against Women (Law 26.485)* expanding existing legislation to explicitly recognize digital violence against women, strengthen victim protections and support, hold digital service-providers accountable, and mandate preventive education and digital literacy programmes to foster safer online environments.

2. Implementation

Legislation on TF VAWG should contain provisions for its effective implementation, evaluation and monitoring.

Legislation should mandate:

- A comprehensive and multisectoral TF VAWG national action plan or strategy
- A budget for its implementation
- The elaboration of rules, regulations and protocols for effective implementation of the law including through intersectoral coordination.

Capacity-strengthening of law enforcement personnel

The ability of legal systems to provide redress for TF VAWG depends heavily on the digital literacy, gender competence and institutional culture of their personnel. Police officers, prosecutors and judges often lack the specialized training to understand the nature, dynamics and impacts of digital harm, resulting in high rates of underreporting, case dismissal and secondary victimization.

Legislation on TF VAWG should:

- Require the provision of mandatory and continuous training on the legal and technical dimensions of TF VAWG – such as the use and admissibility of digital evidence – across all justice sector institutions.
- Provide for training programmes to be developed in consultation with digital rights experts, feminist organizations, violence against women practitioners and victims/survivors to ensure their relevance and responsiveness.

The Office for Internet Safety established by the Icelandic Police Commissioner provides capacity-strengthening to police, prosecutors and emergency call operators, embedding Internet safety and policing into professional and foundational training, including in academic curricula.[32]

3. Monitoring and evaluation

Specific institutional mechanisms to monitor implementation

Legal frameworks on TF VAWG must require independent, gender-sensitive monitoring and evaluation systems based on transparency, participation and intersectionality. Victims/survivors and civil society should help design indicators, assess services and issue recommendations.

Legislation on TF VAWG should:

- Empower human rights, gender equality and data protection bodies to investigate and hold governments and companies accountable
- Establish independent TF VAWG observatories to collect disaggregated data, track trends, evaluate responses and issue public policy recommendations using participatory, intersectional methods
- Ensure oversight bodies can access data, assess public and private actors, publish findings and drive policy change
- Task regulators or similar mechanisms to audit platform practices, involving survivors and experts, and impose sanctions for non-compliance
- Create safe, trauma-informed, multilingual platforms for victims/survivors to report institutional failures, request reviews and challenge responses
- Require annual public reporting on service quality, case resolution, timelines and survivor satisfaction
- Promote gender audits, performance measures, survivor-informed training and gender-transformative leadership
- Involve victims/survivors in feedback mechanisms, panels and evaluations to inform policy and co-design solutions, including anonymous and peer-led reporting
- Nominate focal points within relevant regulatory bodies to monitor TF VAWG, ensure compliance and provide guidance.

Australia's Online Safety Act 2021[33] empowers the national regulator, the eSafety Commissioner, to address various forms of harmful digital conduct. It has the power to issue legally binding notices requiring platforms to take down content that constitutes harmful digital conduct, including some forms of TF VAWG, such as cyberbullying, image-based abuse, cyberstalking and other forms of online harassment and exploitation.

Collection of statistical data

Data are essential to address TF VAWG. It must be reliable, disaggregated by sex and other key characteristics, ethical and privacy-protective to guide effective action.

Legislation should provide for:

- Data collection, access, sharing, transfer, storage and processing practices, from public and private organizations.

The *Ley 11/2007 de prevención y tratamiento integral de la violencia de género*[34] (Galician Law on the Prevention and Treatment of Gender-Based Violence) provides for a special research focus on TF VAWG, to produce knowledge on victims/survivors and perpetrators, the frequency and means through which such violence is committed, impacts on victims/survivors and institutional responses.

4. Definitions

Consent-based legal approach

Legislation on TF VAWG should be based on consent-based definition of the acts, rather than focusing on intent of the perpetrator, while protecting the sexual integrity and privacy of persons.

Legislation should:

- Recognize TF VAWG as a violation of consent linked to structural and gendered harms, not merely privacy infractions
- Incorporate affirmative consent standards in defining violations and liabilities
- Clearly prohibit non-consensual acts, such as sharing of intimate images, use of surveillance tools or identity manipulation
- Inform regulations on user data, facial recognition technologies and algorithmic profiling
- Apply regardless of the nature of the survivor-perpetrator relationship, not excluding aggravating circumstances based on the latter.

The United Kingdom's Crown Prosecution Service issued guidance to specify that, under the UK Online Safety Act (2023),35 and for the first time in the national justice system, an offence – in this instance sharing intimate images or film without consent – is considered a criminal offence, whether or not the perpetrator intended to cause the victim any harm. Prosecutors have the power to apply the law whether the act was committed: without consent; without consent and with intent to cause alarm, distress, or humiliation; and without consent and/or for the purpose of obtaining sexual gratification.[36]

Time-resistant, evidence-based legislation

Legislation should be tech-neutral to ensure it remains time-resistant and applicable despite fast-evolving technologies. Laws must be adaptive and principle-based rather than tied to specific tools. Legislation should be evidence-based and informed by quantitative and qualitative research and data to reflect digital developments and trends and manifestations of TF VAWG. Emerging threats – such as deep-fake pornography, AI-enabled surveillance and algorithmic hate amplification – demand legislative foresight.

Legislation on TF VAWG should:

- Define harm in relation to impact and power asymmetry rather than platform or device
- Acknowledge that harm extends to the emotional, psychological or sexual integrity of a person, the economic, financial, professional or relational situation of the victim
- Include review clauses, flexible definitions of technological means and requirements for periodic stakeholder consultations
- Ensure for the inclusion of incorporating survivor input – especially from marginalized groups – through mechanisms such as sunset clauses and complaint-based review triggers
- Create advisory bodies composed of technologists, feminists, women's safety/ending violence against women practitioners and human rights experts who can support continuous legal adaptation
- Ensure a regular review process to assess the impact of the law and to identify evolving and emerging forms of TF VAWG.

The Finnish Committee for the Future is a Standing Permanent Committee of 17 parliamentarians representing all parties underpinned by the Constitution. An institutionalized foresight system that is explicitly being used to shape technology and gender-sensitive policy, the Committee for the Future serves to ensure deliberation about matters affecting future development, research and the impacts of technological development.[37]

Legal provisions for specific forms of TF VAWG

In addition to providing a broad definition, the law should ensure that characteristics of specific forms of TF VAWG that require complex approaches are addressed.

Legislation on TF VAWG should:

- Explicitly apply to some specific forms of TF VAWG through dedicated provisions targeting forms which are more prevalent or require specific approaches, such as the non-consensual sharing of intimate images, deepfakes, misogynistic hate speech, harassment, threats, extortion, control or spying on virtual activity, unauthorized access to electronic devices or online accounts, theft and non-consensual dissemination of

personal data, actions that violate the sexual integrity of women, including violent pornography and dissemination of images/videos of any form of sexual violence, child sexual exploitation and cyberattacks.

The Take It Down Act (S. 146), enacted as Public Law No: 119-12 on 19 May 2025[38] federal legislation in the United States specifically applies to non-consensual intimate visual depictions, including both authentic photos and artificial intelligence-generated deepfake images that are published online with the intent to harass or harm. The law requires public-facing websites or apps that host user-generated content to remove such intimate images within 48 hours of receiving a valid takedown notice.

5. Prevention

While some of the risk and protective factors for TF VAWG are the same as other forms of VAWG, like harmful gender norms, TF VAWG also comes with unique risk and protective factors, including online communities that normalize misogyny and masculine grievances and enable anonymity.

Legislation on TF VAWG should:

- Require the design and implementation of specifically tailored prevention strategies, including a requirement of education and community-based prevention programmes with a focus on social norm change as well as human rights, digital safety and resilience.

The *Ley 11/2007 de prevención y tratamiento integral de la violencia de género*[39] (Galician Law on the Prevention and Treatment of Gender-Based Violence) establishes several measures to support dedicated TF VAWG prevention efforts. Notably, it provides for awareness-raising campaigns and training for young people on the prevention and identification of behaviours that constitute digital VAWG. Education authorities are tasked with promoting activities in school communities to prevent sexist behaviour and attitudes and gender-based violence, with special attention to digital gender-based violence.

Technology companies must be accountable for preventing and responding to TF VAWG. Automated moderation systems may miss or deprioritize gender-specific harms or misclassify legitimate content that poses no threat. In addition, victims/survivors often report opaque processes and insufficient remedies when engaging with platforms. While platform regulation is important, it often raises questions about free expression, due process and privatized enforcement.

Legislation on TF VAWG should require technology platforms to:

- Ensure effective content moderation mechanisms are in place that do not rely solely on automated systems and include verification through a team of specialized human rights experts and specialists on gender equality and violence against women and girls
- Publish transparent, disaggregated data on content moderation, reports, takedowns, redress processes and appeals
- Adopt safety-by-design approaches in the development and deployment of digital tools and technologies
- Include requirements for AI tools and other digital technologies to undergo checks/impact assessments to ensure they do not reproduce bias or harms before they are released
- Proactively monitor, identify and intervene to halt the spread of harassment campaigns or harmful content
- Ensure ethical and transparent use of algorithms to ensure that they do not amplify harmful or violent content or perpetuate gender bias and stereotypes. Ensure greater cooperation between platforms to trace malicious accounts and identify repeat offenders
- Ensure that risk-assessment frameworks for detecting the activity of extremist groups incorporate indicators to enable the identification of misogynistic networks
- Design technological solutions to prevent TF VAWG in collaboration with women's rights and digital rights experts, VAWG practitioners and victim/survivors.

Germany's 2017 *Netzwerkdurchsetzungsgesetz*[40] or Network Enforcement Act, takes a strict, time-bound approach requiring social media platforms to remove illegal content within 24 hours for clearly unlawful material and within seven days for more complex cases, or face fines of up to 50 million euros for non-compliance.

6. Protection, support and assistance to victims/survivors

Specific protection mechanisms and assistance support must be provided in cases of TFVAWG to address its characteristics. Legislation should provide for the resourcing and equal access and distribution of key resources for victims/survivors' access to justice, including available remedies, legal aid, how to document TF VAWG, digital literacy and mental health support.

Recognition of informal support systems

Feminist collectives, women's rights organizations, community-based support networks, hotlines and digital safety groups play vital roles in responding to TF VAWG through peer-led accountability processes, safety planning and survivor advocacy. These non-formal responses are not a substitute for legal protection but can represent critical mechanisms of care, empowerment and collective resistance.

Legislation should:

- Affirm the legitimacy of alternative responses
- Provide for funding and legal recognition of informal support systems
- Provide for protection from criminalization to sustain informal survivor-centred responses.

Article 16 of the European Union's Directive 2024/1385 on combating violence against women and domestic violence[41] provides that States shall ensure that competent authorities should assess the victim/survivor's individual support needs based on a list of risk factors and individual circumstances due to intersectional discrimination. The competent authorities should further assess dependents' individual support needs.

Removal of harmful content

The prompt identification and removal of harmful content online is a key measure to protect users from abuse, exploitation and other forms of digital harm.

Legislation on TF VAWG should:

- Provide for prompt access to all essential services for survivors of TF VAWG and ensure capacity strengthening on the digital dimensions of VAWG for service-providers
- Ensure that technology companies provide flexible mechanisms as timely interventions to allow for the removal of harmful content before it is too widely spread to be fully removed.

The Online Safety Act 2018 of Fiji[42] ensures that individuals can seek content removal from digital platforms and access support services, including psychosocial support and legal assistance. Victims/survivors can pursue civil remedies through courts for damages resulting from online harm, including emotional distress, reputational damage and financial losses.

Access to justice

Victims/survivors of TF VAWG face the same barriers as victims/survivors of offline violence: stigma, lack of legal remedies, inaccessible reporting mechanisms and widespread impunity. The anonymity of perpetrators and the transnational nature of the crimes create additional barriers for access to justice and support services. Support and resources should be provided to all victims/survivors, recognizing the unique and often hidden trauma associated with TF VAWG.

Legislation on TF VAWG should:

- Request the provision to victims/survivors of specific information on their rights and the procedures, including protective measures for TF VAWG cases;
- Call for victims/survivors to be connected with appropriate support services, e.g., health and social services;
- Call for the creation of digital complaints' portals to enable victims/survivors to report harm in a safe, accessible, and culturally sensitive manner.

The Electronic Cybercrime Report and Management system was developed by the Korean National Police Agency to facilitate the reporting of cybercrime, online case registration and case assignment and delivery of response. This tool helps victims/survivors prepare relevant documents, thus reducing the time taken to visit police stations. It also has an integrated Chabot function to respond to queries victims/survivors may have and uses AI technology to expedite the monitoring/tracking of illegally filmed materials and deep-fake videos.[43]

Digital protection orders

Protection orders are a vital legal tool to provide safety, recognition and support to victims/survivors while holding perpetrators accountable. In cases of TF VAWG, it is critical that protection orders also cover digital environments and are not limited to physical spaces.

Legislation on TF VAWG should:

- Extend traditional protection orders for victims/survivors of both domestic violence and non-partner violence to digital spaces to expand protection, both offline and online.

South Africa's Domestic Violence Amendment Act of 2021[44] expands protections under the original Domestic Violence Act of 1998,[45] recognizing digital violence as a form of domestic abuse. Victims can apply for protection orders electronically, reducing barriers for those in urgent need of legal protection. The act introduces the concept of a 'domestic violence safety monitoring notice', allowing closer monitoring of compliance with protection orders. The police and courts can issue emergency digital protection orders, restricting abusers from contacting victims using any digital means.

7. Investigation

Investigating TF VAWG requires specialized protocols for the collection, preservation and interpretation of digital evidence. Standard operating procedures are key to ensure consistent handling of cases and preservation of critical information.

Legislation on TF VAWG should:

- Provide for the adoption by national police and prosecutorial bodies of TF VAWG-specific investigative protocols that address the preservation of metadata, coordination with online platforms and survivor safety throughout the investigation
- Call for cooperation frameworks with digital platforms, which are essential to ensure timely content takedown, information requests and data preservation
- Require that these tools include transparency requirements, due process guarantees and respect for users' privacy and rights.[46]

In the Philippines, the Safe Space Act, also known as the Republic Act No. 11313,[46] was passed in 2018 to address gender-based sexual harassment, with the explicit inclusion of 'gender-based online sexual harassment' through a dedicated definition and section. The law clearly identifies the Philippine National Police Anti-Cybercrime Group as the law enforcement body responsible for implementation. It is tasked with providing adjusted services, including complaint filing, the development of an online reporting mechanism and perpetrator accountability. Another police unit, the Cybercrime Investigation and Coordinating Centre, is tasked with monitoring and penalization measures.

8. Legal proceedings and evidence

Traditional legal processes are not adapted to the specificity of TF VAWG. Collection of digital evidence, anonymity and the technical complexities of online platforms pose additional challenges. Adapting proceedings ensures rapid, survivor-centred protection, proper handling of digital evidence and accountability for perpetrators, while addressing the unique psychological and social impacts of technology-facilitated abuse.

Legislation on TF VAWG should:

- Update evidentiary frameworks to ensure admissibility and safe conservation of digital evidence related to TF VAWG
- Institutionalize survivor protection measures during legal proceedings. These may include the use of pseudonyms, closed hearings, trauma-informed questioning, protective orders and access to psychosocial support.

In 2023, Nigeria passed the Evidence Act (Amendment) 2023 (amending the Evidence Act 2011),[47] which introduced provisions recognizing "electronic records", "digital signatures" and "audio-visual deposition", among others, for admissibility of evidence. The Amendment expands the definition of admissible electronic evidence, with Section 2 defining "electronic record" to mean data, record or data-generated image or sound stored, received or sent in electronic form.

9. Sentencing and penalties

Adapting sentencing ensures that punishment of perpetrators is proportionate to the scale and impact of TF VAWG and deters repeat offenses. Penalties can also directly apply to the specificities of TF VAWG perpetration, by restricting access to or use of online platforms or digital tools.

Legislation on TF VAWG should:

- Provide for penalties adapted for individuals and legal or corporate entities found guilty of TF VAWG
- Include traditional penalties, such as fines, as well as ones specifically related to the nature of the offence, such as the revocation of licenses or franchises
- Provide for the development of compulsory courses for perpetrators focused on gender equality and integrity, which can be ordered by means of probation of the sentence.
- Define aggravating circumstances, including based on evidence of intent to harm or economic profit – notably for private companies.

In 2018, Brazil adopted Law No. 13.722/2018,[48] which introduced significant amendments to both the *Lei Maria da Penha* (Law No. 11.340/2006)[49] and the Brazilian Penal Code (Decree-Law No. 2.848/1940)[50] aimed at addressing violations of women's privacy and TF VAWG. Penalties for offenders are stipulated for non-consensual distribution of intimate content, cyberstalking and digital harassment, sexual extortion and coercion in the digital space, and virtual sexual exploitation. Stronger penalties apply to aggravating crimes, such as cases of extortion or blackmail, or where minors are involved.

10. Civil lawsuits

Civil law can offer more accessible, flexible and survivor-controlled avenues than criminal prosecution. Civil remedies are essential to ensure victims/survivors are empowered within the justice system by providing them with the option to seek alternative proceedings should victims/survivors not wish to pursue this avenue or in cases of offences that may not meet the criminal threshold.

Legislation on TF VAWG should:

- Provide for civil remedies including restraining orders, compensation claims for emotional distress, defamation suits and data protection complaints
- Provide avenues for victims/survivors to seek civil injunctions to compel content removal or prevent ongoing harassment.

In California, Civil Code § 1708.86 gives individuals a private right of action against anyone who creates or shares a sexually explicit "altered depiction" without the depicted person's consent.[51] An "altered depiction" refers to a performance by the individual that has been digitally modified.

11. Administrative remedies and data governance

Administrative bodies, such as data protection authorities, equality commissions and telecommunications regulatory bodies offer additional pathways for redress. Administrative procedures can complement criminal and civil law by focusing on systemic remedies and institutional accountability.

Legislation on TF VAWG should provide for:

- Complaints mechanisms regarding unauthorized data-sharing, discriminatory content moderation, or platform negligence
- Data protection frameworks with remedies to challenge the collection and dissemination of intimate content
- Recourse mechanisms to allow victims/survivors and civil society to escalate unresolved cases to independent oversight bodies with authority to mediate, recommend actions and drive systemic reform

- The creation of mechanisms to institutionalize the collaboration between data authorities and gender justice bodies on TF VAWG cases.

On 26 June 2025, Brazil's Federal Supreme Court redefined the civil liability of digital platforms by declaring the partial unconstitutionality of Article 19 of the *Marco Civil da Internet* (Law No. 12.965/2014), thereby introducing a new "duty of care" standard.[52] Under this framework, platforms are required to act proactively to remove serious illegal content when it circulates widely, even without prior judicial or user notification. Failure to act diligently may result in civil liability. The Court provided an exhaustive list of serious offences triggering this proactive duty, including crimes against women.

Integrating the actions laid out in this policy brief, and examples of good practices, will be key to preventing and responding to TF VAWG in a comprehensive manner to strengthen access to justice and end impunity.

Endnotes

1 Santagostino, R. and M. Elefante. 2023. "Protecting women and girls from cyber harassment: a global assessment." World Bank Blogs. 27 November. https://blogs.worldbank.org/en/developmenttalk/protecting-women-and-girls-cyber-harassment-global-assessment

2 World Bank. 2024. Women's Safety.

3 Dunn, S. 2022. Addressing Gaps & Limitations in Legal Frameworks and Law Enforcement on Technology-Facilitated Violence against Women. UN Women Expert Group Meeting. "Innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls." October.

4 The Supplement was produced by UN Women in collaboration with the Association for Progressive Communications through global consultations. It draws on desk research and in-depth assessments in 25 countries, validated by local experts. Research questions informed consultations with academics, civil society, victims/survivors' groups, governments and international organizations, supported by five regional expert meetings and expert reviewers.

5 United Nations General Assembly (UNGA). 2024. Report of the Secretary-General on the Intensification of efforts to eliminate all forms of violence against women and girls: technology-facilitated violence against women and girls. A/79/500.

6 UN Women. 2022. Technology-facilitated Violence against Women: Towards a common definition – Report of the meeting of the Expert Group. 15-16 November 2022, New York.

7 See notably the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) and General Recommendation 35; the International Covenant on Civil and Political Rights (ICCPR) on the right to life, liberty, privacy and freedom from cruel, inhuman or degrading treatment; the International Covenant on Economic, Social and Cultural Rights (ICESCR) on the rights to health, education and participation; and the Universal Declaration of Human Rights (UDHR) on the rights to security, freedom of expression and privacy.

8 Commission on the Status of Women. 2023. Innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls: CSW 67 Agreed Conclusions.

9 UNGA. 2023. Resolution 78/213 on Promotion and Protection of Human Rights in the context of digital technologies.

10 UN Women. 2025. Normative Advances on Technology-Facilitated Violence Against Women and Girls.

11 United Nations Office for Digital and Emerging Technologies. Undated. "Global Digital Compact".

12 UNGA. 2024. Resolution 79/152: Intensification of efforts to prevent and eliminate all forms of violence against women and girls: the digital environment.

13 United Nations Office on Drugs and Crime (UNODC). Undated. United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes.

14 UN Women 2025.

15 EUR-Lex. 2024. Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence.

16 See UNGA 2024. A/79/500.

17 UNGA. 2022. Report of the Secretary-General on the Intensification of efforts to eliminate all forms of violence against women and girls. A/77/302.

18 See United Nations Population Fund (UNFPA). 2022. Policies for tackling tech-facilitated gender-based violence: multi-stakeholder perspectives and learnings from around the world.

19 See United Nations Office of the High Commissioner for Human Rights (OHCHR). 2021. "Moderating online content: fighting harm or silencing dissent?" 23 July. https://www.ohchr.org/en/stories/2021/07/moderating-online-content-fighting-harm-or-silencing-dissent

20 Dunn, S. 2022. Addressing Gaps & Limitations in Legal Frameworks and Law Enforcement on Technology-Facilitated Violence against Women. UN Women Expert Group Meeting "Innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls."

21 OHCHR. 2021. Statement by Irene Khan, Special Rapporteur on the promotion and protection of freedom of opinion and expression.

22 OHCHR. 2025. Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression. A/80/341.

23 Internet Society. 2020. Fact Sheet: Understanding Encryption: The Connections to Survivor Safety

24 Jankowicz, N. et al. 2024. It's everyone's problem: mainstreaming responses to technology-facilitated gender-based violence; Marganski, A. and L. Melander. 2021. Technology-Facilitated Violence against Women and Girls in Public and Private Spheres: Moving from Enemy to Ally.

25 OECD. 2025. Mapping policy response to technology-facilitated gender-based violence in the G7 countries.

26 Dunn 2022.

27 Ibid.

28 UNICEF, UNFPA & Save the Children Technology-facilitated gender-based violence: Considerations across the life course

29 Ibid.

30 See Government of Argentina. 2023. "Olimpia Law" [in Spanish]

31 ALiGN. 2024. Digital sexual violence against women in Mexico: Role of the Olimpia Law in transforming underlying gender norms.

32 See Ministry of Interior, Iceland. 2015. Icelandic National Cyber Security Strategy 2015–2026.

33 See Federal Register of Legislation, Australia. 2021. Online Safety Act 2021. https://www.legislation.gov.au/C2021A00076/latest/text

34 See Autonomous Community of Galicia, Spain. 2022. Law 15/2021 [In Spanish] https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-3412https://www.boe.es/diario_boe/txt.php?id=BOE-A-2007-16611

35 See Government of the United Kingdom. 2023. Online Safety Act.

36 See Crown Prosecution Service, United Kingdom. 2024. "Illegal sexual behaviour online, including sharing and threatening to share intimate images and cyberflashing targeted in new CPS guidance." 31 January. https://www.cps.gov.uk/cps/news/illegal-sexual-behaviour-online-including-sharing-and-threatening-share-intimate-images

37 See Koskimaa, V. 2025. Ten – the Finnish National Foresight System. Cambridge University Press.

38 United States Congres. 2025. Public Law No: 119-12.

39 Autonomous Community of Galicia, Spain. 2022. Law 15/2021.

40 Bundesministerium der Justiz und für Verbraucherschutz. 2017. Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG).

41 EUR-Lex. 2024. Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence.

42 Office of the Attorney-General, Fiji. 2018. Online Safety Act 2018.

43 Information provided by the Korean National Police Academy.

44 Government of South Africa. 2022. Domestic Violence Amendment Act, 2021. Government Gazette.

45 Government of South Africa, 2023. Domestic Violence Act No. 116 of 1998.

46 The LAWPhil Project. 2018. Seventeenth Congress, Third Regular Session. Republic Act No. 11313.

47 World Intellectual Property Organization (WIPO). 2023. Evidence (Amendment) Act, 2023, Nigeria.

48 Government of Brazil. 2018. Law No. 13.722/2018. [Portuguese].

49 The law is named after journalist Rose Leonel, who became an activist after her intimate photos were non-consensually shared online.

50 Government of Brazil. 2006. Decree Law No. 2.848/1940. [Portuguese].

51 Find Law. 2023. California Code, Civil Code – CIV § 1708.86.

52 Supreme Federal Tribunal, Brazil. 2025. RE. 1.037.396 (Tema 987) e 1.057.258 (Tema 533) [Portuguese]

220 East 42nd Street
New York, New York 10017, USA
Tel: 646-781-4400
www.unwomen.org

UN WOMEN

FOR ALL WOMEN AND GIRLS