GLOBAL TRENDS TO PREVENT AND RESPOND TO TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN AND GIRLS: A COMPENDIUM OF EMERGING PRACTICES

SVRI sexual violence research initiative

UN WOMEN

Acknowledgments

This research paper has been developed by the Ending Violence against Women and Girls Section of the United Nations Entity for Gender Equality and the Empowerment of Women (UN Women), in collaboration with the Sexual Violence Research Initiative (SVRI) and its Global Community of Practice on Technology-Facilitated Gender Based Violence (TF GBV CoP).

UN Women and SVRI thank Leonie Tanczer from the University College London, Misha'ari Weerabangsa from Delete Nothing, Merrin Muhammed Ashraf from IT for change, Donald Flywel from the University of Livingstonia, Loes Loning from Rutgers, Ogechi Ikeh from Ogechi & Sam Ikeh Foundation, Laura McVey from the eSafety Commissioner, and Alexandra De Filippo from SVRI TF GBV CoP, for their inputs.

UN Women and SVRI. 2025. Global Trends to Prevent and Respond to Technology-Facilitated Violence against Women and Girls: A Compendium of Emerging Practices. New York: UN Women.

Copy editing: Gretchen Luchsinger

Design: The Visual Agency

The views expressed in this publication are those of the authors and do not necessarily represent the views of UN Women, the United Nations or any of its affiliated organizations.

This product has been made possible by the generous financial support of the The Spanish Agency for International Development Cooperation (AECID).

aecid
Spanish Agency
for International Development
Cooperation

GLOBAL TRENDS TO PREVENT AND RESPOND TO TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN AND GIRLS: A COMPENDIUM OF EMERGING PRACTICES

Ending Violence against Women and Girls Section
UN Women
New York, 2025

FOR **ALL**
WOMEN
AND GIRLS

TABLE OF CONTENTS

ACRONYMS

CSW	Commission on the Status of Women
HRC	Human Rights Council
ICT	Information and communication technology
LGBTQI+	Lesbian, gay, bisexual, transgender, queer/questioning, intersex plus
NGO	Non-governmental organisation
SVRI	Sexual Violence Research Initiative
TF VAWG	Technology-facilitated violence against women and girls
UNGA	United Nations General Assembly
VAWG	Violence against women and girls

EXECUTIVE SUMMARY

Advances in digital technologies coupled with globalization have fundamentally transformed human interactions, enabled new forms of communication and facilitated the sharing of information across borders. Despite their transformative nature, digital technologies pose risks of spreading misinformation and violence. They have ignited new forms and patterns of violence against women and girls (VAWG) due to unique characteristics, including a vast reach and scale, the rapid dissemination of information, the ease of communication, and anonymity, automation and affordability.[1]

The term technology-facilitated violence against women and girls (TF VAWG)[2] captures both existing forms of VAWG exacerbated by technologies and new forms that have emerged through technologies in online and offline spaces. TF VAWG forms a continuum of multiple, recurring and interrelated forms of violence operating across multiple platforms and media, including social media, messaging applications, emails, and smart devices and tools. TF VAWG is also used to perpetrate offline VAWG. For example, technologies are used to monitor and control women's movements, such as through devices including smart watches or video doorbells that connect to smartphones. TF VAWG encompasses various harmful behaviours, including cyberstalking, doxing, non-consensual intimate image abuse, deepfakes and unwanted messages or posts.

Global Trends to Prevent and Respond to Technology-Facilitated Violence against Women and Girls: A Compendium of Emerging Practices (referred to as the Compendium moving forward) compiles, reviews and organizes emerging practices to address TF VAWG. It is a living document that highlights different approaches, tactics and strategies adopted by governments, civil society, the United Nations and technology companies.[1] Through a review and categorization of existing resources as well as an identification of gaps, the Compendium provides a tool for policymakers, advocates and practitioners addressing TF VAWG.

The Compendium was developed in collaboration with experts and practitioners in VAWG and TF VAWG, including with the global community of practice established by the Sexual Violence Research Initiative (SVRI), to uphold accuracy and relevance. It details trends and contextual differences, offering a nuanced understanding of TF VAWG interventions across different platforms and contexts. The practices presented show the importance of establishing comprehensive frameworks and interventions based on multistakeholder collaboration and a shared understanding of how technologies can and are used to perpetuate or facilitate VAWG. The Compendium overall seeks to increase knowledge and encourage efforts to prevent and respond to TF VAWG.

[1] The inclusion of practices in this Compendium does not mean that they or the companies or organisations that are leading them are endorsed by UN Women or the United Nations.

INTRODUCTION

BACKGROUND

In today's hyperconnected world, the digital revolution has transformed every aspect of our lives, offering unprecedented opportunities for communication, learning, earning and activism. It has played a critical role in women's collective organizing and advocacy to end VAWG and gender discrimination, and become a powerful tool to connect feminist movements.[3] Yet the digital realm has also become another setting where women and girls, in all their diversity, experience violence.[4]

TF VAWG is a pervasive threat that transcends borders and invades the most personal aspects of women's lives. Increased access to and use of information communications technology (ICT) and digital tools has exacerbated existing forms of VAWG, including sexual harassment, and given rise to new forms,[5] such as non-consensual image-sharing, zoom-bombing, doxing, deepfake videos and gendered disinformation. As technology, digital tools and applications evolve, so do the forms and patterns of violence. TF VAWG is not confined to any single platform or medium; it operates across social media, messaging apps, emails, gaming, educational and professional platforms, global positioning systems and smart devices, often leaving victims-survivors vulnerable, isolated and without recourse.

Despite limited globally comparable data, studies show that technology-facilitated violence is widespread. Prevalence among women ranges from 16 to 58 per cent.[6] Younger women,[7] particularly in Gen Z (born between 1997 and 2012) and Millennials (born between 1981 and 1996), are more at risk; girls face severe impacts.[8] In 2024, 97 per cent of child sexual abuse imagery where the victim's sex was recorded showed girls only. Often, images were "self-generated" under coercion, grooming or extortion, most commonly targeting 11–13 year-olds, with a sharp rise among 7–10 year-olds.[9] Around 40 per cent of girls report harassment at least monthly and 11 per cent daily or almost daily, echoing earlier findings that 58 per cent of girls have personally experienced online abuse.[10]

Related harms are escalating, with a 192 per cent annual rise in online enticement reports in 2024 and over 26,000 cases of financial sextortion in 2023.[11] Perpetrators are often known to the victim-survivor, and risks are heightened for women politicians, journalists, human rights and environmental defenders, feminist activists, and women and girls perceived as challenging gender norms and patriarchal structures, including LGBTQI+ (lesbian, gay, bisexual, transgender, queer/questioning, intersex plus) individuals and those with limited access to digital tools and literacy. TF VAWG disproportionately impacts women and girls. The most affected groups include women facing multiple and intersecting forms of discrimination, such as racialized women and women belonging to religious or ethnic minorities,[12] young women,[13] poor women[14] and women with disabilities.[15]

The urgency of this issue cannot be overstated. TF VAWG is not only confined to online spaces. Virtual reality and the metaverse are creating new digital spaces for misogyny and sexual violence, which are further exacerbated by the growth of artificial intelligence, such as deepfake sexual videos.[16] Digital platforms are being exploited to spread gendered misinformation and disinformation, which is fuelling extreme misogyny and anti-gender rhetoric aimed at pushing back against progress made on gender equality. The manosphere opens even more scope for TF VAWG. It is understood as a loose network of communities focused on issues relating to men. But these communities are predominantly male extremist and incel groups[17] engaged in harmful rhetoric against women, girls, LGBTQI+ individuals and other groups. They reinforce violent behaviour online and offline.[18]

As evidence grows on the severity and scale of TF VAWG, the need for targeted and effective interventions has become more urgent. Rapidly evolving technology necessitates robust and flexible legal, policy and accountability frameworks. Addressing TF VAWG requires a comprehensive approach, including laws consistent with international human rights law; regulatory frameworks that are effectively implemented; greater investments in quality research guided by priorities identified by researchers and practitioners; robust evidence-based programming for prevention and response, including through technology companies, along with actions to improve transparency; and partnerships among governments, technology providers, and civil society and women's rights organizations.

PURPOSE AND SCOPE

The Compendium provides an overview of emerging practices and interventions by different actors, with a focus on governments, civil society organizations and technology companies. It showcases select laws, policies, programmes and initiatives, and highlights global trends in addressing, preventing and responding to TF VAWG.

WHO IS THE COMPENDIUM FOR?

The Compendium is designed for governments, policymakers, researchers, civil society organizations, technology companies and other stakeholders engaged and interested in addressing TF VAWG.

HOW WAS THE COMPENDIUM DEVELOPED?

A multi-step process to develop the Compendium began with comprehensive data collection. This exercise, conducted over one year, used a combination of database-driven research, literature reviews and analysis of government reports, predominantly in English and Spanish. Data were triangulated from various sources, including UN Women's **Global Database on Violence Against Women**; Member State submissions to reports of the United Nations Secretary-General and the review of the thirtieth anniversary of implementation of the Beijing Declaration and Platform for Action; the global community of practice established by the **Sexual Violence Research Initiative** (SVRI), reports from civil society organizations, intergovernmental bodies and other United Nations entities; and academic and grey literature.

Objectives of the Compendium	
Centralization of emerging practices	To create a single, accessible resource that consolidates emerging practices, including select laws, policies, programmes and initiatives aimed at preventing and responding to TF VAWG.
Facilitating collaboration	To highlight successful partnerships and cooperative efforts among governments, civil society organizations, technology companies and other stakeholders to encourage cross-sector collaboration.
Supporting policy and programmatic action	To provide examples of different practices to prevent and respond to TF VAWG, and to inspire action by policymakers, advocates and practitioners in developing new or reviewing existing strategies, policies and frameworks to prevent and respond to TF VAWG.
Evolve with evidence and experience	To serve as a living resource that will be refined and expanded as new data, evaluations, guidance and innovative approaches become available. By capturing current trends while remaining adaptable to future developments, the Compendium aims to deepen understanding and support interventions that are evidence-informed, contextually relevant, and capable of achieving meaningful, sustained reductions in violence.

Once collected, interventions were categorized based on several variables, including their nature, scope and source, and clustered around specific intervention areas, namely: normative frameworks, legislative measures, and prevention and response mechanisms. Interventions were then assessed based on specific criteria of relevance and impact. These included a focus on directly addressing TF VAWG, comprising specific forms such as digital violence, including online harassment and non-consensual intimate image-sharing. Geographic diversity was a key consideration, with efforts to include interventions from different regions to capture how TF VAWG manifests and is being addressed across cultural and socioeconomic contexts. Additionally, the criteria emphasized innovations, particularly those leveraging new technologies, and prioritized sustainability by highlighting initiatives designed for long-term impact and scalability. The Compendium aims to provide a balanced perspective by presenting interventions by governments, civil society organizations and technology companies.

The Compendium uses the term "emerging practices" to refer to new, innovative or evolving strategies or approaches that have been developed, piloted and implemented to address TF VAWG. These may not yet have the strong base of evidence required to define them as "promising" or "good" practices. They may require further monitoring and assessment before being considered for replication and/or scale-up.

LIMITATIONS

The Compendium is limited in scope due to its reliance on publicly available sources. Many interventions by governments, civil society organizations and technology companies may currently remain unpublished or inaccessible. In line with the definition of emerging practices above, the impact of these interventions is generally not fully understood. Many are recent; most have not yet been properly evaluated. The Compilation serves as a starting point for at least understanding current efforts to strengthen responses and prevent TF VAWG, while recognizing the need for more comprehensive and diverse data collection and analysis in the future.

HOW TO USE THE COMPENDIUM

The Compendium should be read and understood as a dynamic, evolving document. It is not intended to encompass all interventions but rather curates interventions to illustrate different practices and approaches adopted by diverse stakeholders across different contexts. Examples were carefully selected to highlight best or emerging practices for each trend. As more information becomes available, the Compendium will be updated to reflect new data, evaluations and innovations, keeping it relevant and responsive to the fast-changing nature of technology-facilitated violence.

Some initiatives featured in the Compendium address multiple aspects of prevention and response, or operate across different sectors (for example, digital tools that also function as reporting mechanisms). For ease of navigation, each example has been placed under the subsection that best reflects its primary function or where the bulk of its work is situated. This categorization is not intended to be exhaustive, but rather to provide readers with a clear structure to explore emerging practices.

The Compendium can be used based on readers' interests and needs. Each chapter outline identifies the most relevant content.

OVERVIEW OF CHAPTERS

The first chapter provides an overview of the global and regional normative framework that sets standards for addressing TF VAWG. The chapter highlights progress in global understanding of TF VAWG and efforts to address it.

The second chapter delves into legislative efforts by countries to address TF VAWG. It highlights different approaches by national and subnational lawmakers.

The third chapter focuses on initiatives and strategies to prevent TF VAWG. These include educational programmes, awareness-raising campaigns, efforts to shift social norms and technological solutions.

The fourth chapter examines response mechanisms, looking at support systems and resources for TF VAWG victims-survivors. It explores the roles of law enforcement, judicial systems and technology companies in upholding accountability.

The fifth chapter provides a summary and offers ways forward, presenting recommendations on crucial actions to create safe and equitable digital spaces for women and girls and marginalized groups, free from violence and harm.

Photo: UN Women/WCARO

1

OVERVIEW OF GLOBAL AND REGIONAL NORMATIVE FRAMEWORKS ON ADDRESSING TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN AND GIRLS

Photo: UN Women/Ploy Phutpheng

Global and regional norms increasingly recognize TF VAWG as part of the continuum of gender-based violence. Early instruments on ending violence against women predated today's digital harms but acknowledged the gendered impact of technological change. The 1995 Beijing Declaration and Platform for Action urged measures to mitigate technology's effects on women and to ensure equal participation in digital developments.[19] As evidence on TF VAWG has accumulated, intergovernmental bodies have begun to integrate digital harms more explicitly into women's rights agendas.

Over the past decade, global and regional frameworks have moved from implicit recognition to more direct articulation.[20] They trace a clear trajectory: Early attention to the gendered implications of technology has evolved into increasingly specific global and regional commitments that locate TF VAWG within human rights and digital governance agendas. Further, they conceptualize it as part of a continuum of violence requiring prevention, protection and accountability across interconnected online and offline environments.[21]

1. GLOBAL NORMATIVE FRAMEWORKS

● Convention on the Elimination of All Forms of Discrimination against Women

2017: While the 1979 Convention on the Elimination of All Forms of Discrimination against Women[22] did not address TF VAWG, in 2017, **General Recommendation No. 35**[23] identified it as an emerging form of gender-based violence, thereby clarifying that such new manifestations fell within the treaty's scope.

● Agreed conclusions of the Commission on the Status of Women

2013: The Commission on the Status of Women, for the first time, clearly recognized that ICT and social media could be used to perpetrate violence against women and girls, and urged the development of mechanisms to address it.[24]

2023: The Commission's agreed conclusions on innovation and technological change[25] called for a policy of zero tolerance against all forms of violence against women in the digital sphere, including harassment, stalking, bullying, surveillance and extortion. They stressed the need to develop and/or strengthen legislation that protects women and girls from TF VAWG.

● Resolutions of the United Nations General Assembly

2022: General Assembly Resolution 77/193 on the intensification of efforts to eliminate all forms of violence against women and girls: gender stereotypes and negative social norms[26] for the first time explicitly urged States to address the risks posed by digital technologies.

2022: General Assembly Resolution 77/194 on trafficking in women and girls[27] acknowledged the role of ICT in facilitating trafficking.

2024: At the **Summit of the Future**, UN Member States adopted the **Global Digital Compact,**[28] an annex to the **Pact for the Future**, as the first comprehensive framework for global governance of digital technologies and artificial intelligence. The Compact acknowledges the potential for harm posed by digital platforms and calls for secure online spaces, the development of standards and guidelines to prevent harmful content, and national legislation aligned with international human rights law.

2024: General Assembly Resolution 79/152 on the intensification of efforts to eliminate all forms of violence against women and girls: the digital environment[29] urged Member States to enact and enforce legislation to prevent, investigate and prosecute online violence; strengthen survivor-centred support, including confidential reporting and referral pathways; and ensure women and girls have access to digital literacy and online safety skills. It called on States to avoid the use of artificial intelligence systems that cannot be operated in compliance with human rights law or that create disproportionate risks, and to strengthen cooperation with women's rights organizations and the private sector in building safe digital spaces.

2024: General Assembly Resolution 79/154 on trafficking in women and girls[30] further emphasized the misuse of ICT to facilitate trafficking, urging enhanced international cooperation to combat online trafficking, improve mechanisms to detect and remove exploitative content, and integrate survivor-centred, gender-responsive approaches into anti-trafficking strategies.

● United Nations Convention against Cybercrime

2024: The General Assembly adopted the United Nations Convention against Cybercrime.[31]

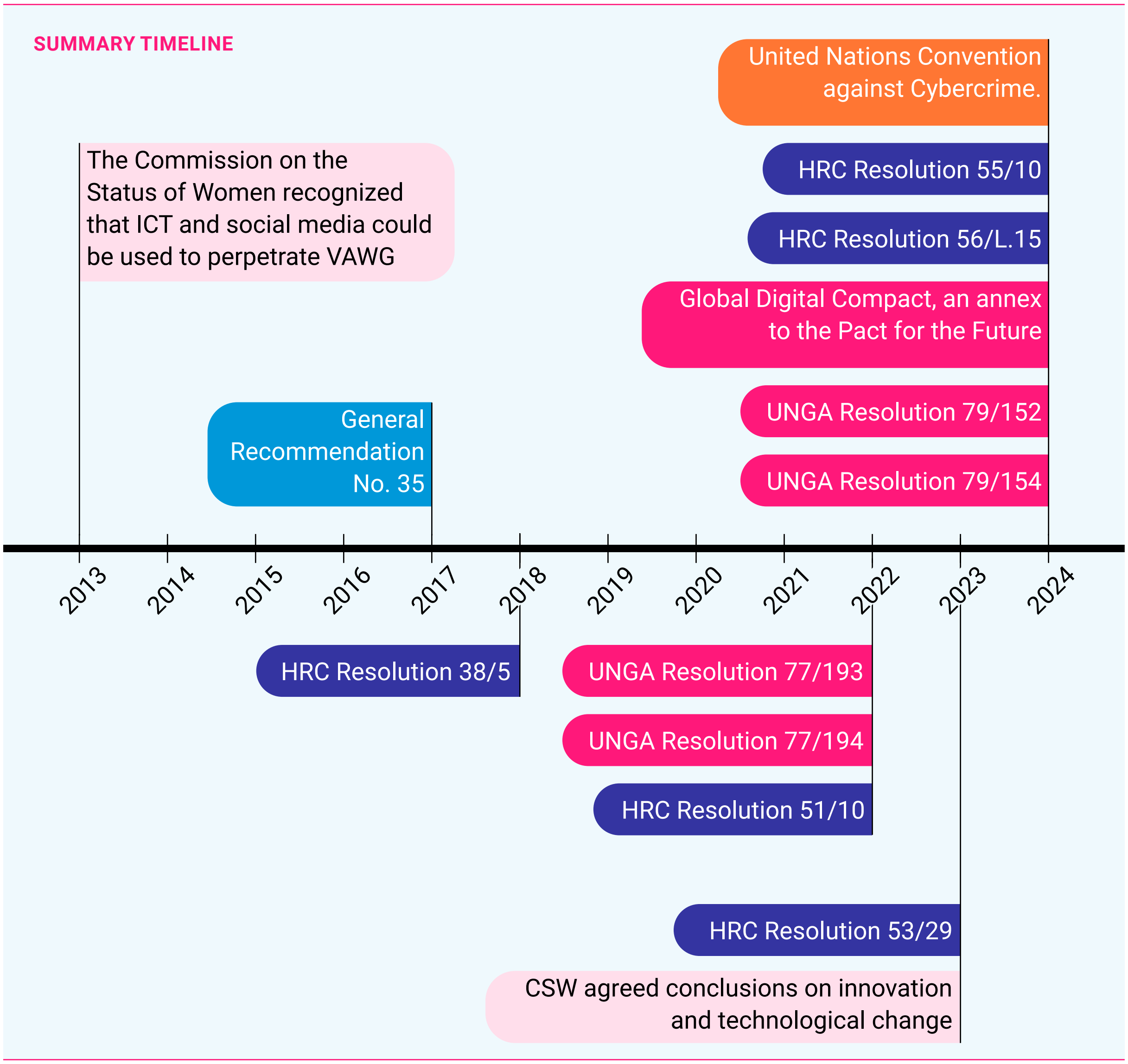
● United Nations Human Rights Council

2018: Resolution 38/5 called for State action to prevent TF VAWG.[32]

2022: Resolution 51/10 on countering cyberbullying called for strengthening legal frameworks.[33]

2023: Resolution 53/29 focused on the impact of emerging technologies and called for better safeguards against TF VAWG.[34]

SUMMARY TIMELINE



The Commission on the Status of Women recognized that ICT and social media could be used to perpetrate VAWG

General Recommendation No. 35

HRC Resolution 38/5

UNGA Resolution 77/193

UNGA Resolution 77/194

HRC Resolution 51/10

HRC Resolution 53/29

CSW agreed conclusions on innovation and technological change

United Nations Convention against Cybercrime.

HRC Resolution 55/10

HRC Resolution 56/L.15

Global Digital Compact, an annex to the Pact for the Future

UNGA Resolution 79/152

UNGA Resolution 79/154

2024: Resolution 55/10 called attention to the role of disinformation in exacerbating online violence,[35] and resolution 56/L.15 called for a comprehensive study to better understand TF VAWG and develop solutions with stakeholder involvement.[36]

2. REGIONAL NORMATIVE FRAMEWORKS

Africa

In 2022, the African Commission on Human and Peoples' Rights adopted a specific resolution on the protection of women against digital violence in Africa.[37] It notably called on States to review and amend their laws to include digital violence, and to expand their definitions of gender-based violence to include forms of digital violence such as cyberharassment, cyberstalking, sexist hate speech and others. The Commission urged States to conduct research on digital violence, develop educational campaigns addressing its root causes, and implement training programmes for practitioners and professionals supporting victims-survivors. Additionally, it called for measures to protect women journalists and for the revision of vague and overreaching surveillance laws that disproportionately impact them.

In 2025, the African Union adopted the Convention on Ending Violence Against Women and Girls,[38] a legally binding framework for the prevention, elimination and effective response to all forms of violence against women, including those perpetrated on online platforms.

Asia

Adopted in 2013, the Association of Southeast Asian Nations (ASEAN) Declaration on the Elimination of Violence Against Women and Elimination of Violence Against Children[39] explicitly recognizes that violence against women and children can also happen in "cyberspace". It calls for strengthening legislation and adopting a holistic approach to eliminate all forms of violence. The ASEAN Regional Plan of Action on the Elimination of Violence Against Women (2016–2025)[40] subsequently called on ASEAN member States to "review and revise national laws in recognition and consideration of new and emerging forms of [violence against women], such as sexual violence against women in cyberspace". A midterm review suggested prioritizing the development of guidelines to support various groups of vulnerable women and address different forms of violence, including underrecognized types such as cyberviolence.[41]

Europe

In 2021, the Council of Europe Group of Experts on Action against Violence against Women and Domestic Violence, the treaty body of the 2011 Istanbul Convention,[42] issued General Recommendation No. 1 on the Digital Dimension of Violence against Women.[43] It recognizes "the perpetration of violence against women online or with the help of technology as a continuity of the different forms of such violence that affects and exacerbates women and girls' experiences of gender-based violence against women to an alarming extent". The group further clarified that "non-consensual image or video sharing, coercion and threats, including rape threats, sexualised bullying and other forms of intimidation, online sexual harassment, impersonation, online stalking or stalking via the Internet of Things (IoT) as well as psychological abuse and economic harm perpetrated via digital means against women and girls all come under the [...] definition [of violence against women set out in Article 3a of the Istanbul Convention]". The recommendation called on States Parties to implement prevention measures such as digital literacy programmes, protection mechanisms such as victim-survivor support services, and prosecution strategies to strengthen legal frameworks and law enforcement. It emphasized the need for coordinated policies among governments, civil society and the private sector to combat digital violence effectively.

In 2022, the European Union passed the Digital Service Act,[44] which establishes a comprehensive regulatory framework for online platforms, digital services and intermediaries operating in the European Union. The Act requires platforms to establish measures to counter the spread of illegal goods, services or content online, such as mechanisms for users to flag such content and for platforms to cooperate with "trusted flaggers".[45] Specifically, providers of very large online platforms "used for the dissemination to the public of pornographic content" are required to ensure that victims can effectively exercise their rights to have content representing non-consensual sharing of intimate or manipulated material removed "through the rapid processing of notices and removal of such content without undue delay".

In May 2024, the European Parliament and Council adopted Directive (EU) 2024/1385,[46] the European Union's first comprehensive legal instrument to combat violence against women and domestic violence. Crucially, it brings online harms explicitly within its scope. The Directive criminalizes serious forms of cyberviolence across all Member States – namely, the non-consensual sharing of intimate or manipulated images, cyberstalking, cyberharassment and cyberincitement to hatred or violence based on gender. Member States are required to transpose these provisions into national law by June 2027, ensuring these online offences are uniformly addressed across the Union. Beyond defining these cyberoffences, the Directive also mandates robust victim protection, access to justice, prevention measures and coordination among authorities. It anchors digital gender-based violence within a broader framework of gender-sensitive legal and institutional responses.

Latin America and the Caribbean

In 2022, the follow-up mechanism to the 1994 Inter-American Convention on the Prevention, Punishment and Eradication of Violence Against Women (Belém do Pará Convention)[47] clarified the application of the Convention to cyberviolence against women and girls through a dedicated report.[48] The mechanism is currently developing a model law for the region to prevent, punish and eradicate TF VAWG, which would provide countries with legislative guidance to address the issue effectively.[49]

Pacific

In 2023, the first regional symposium on cyber-violence, Safe and Equal Online Spaces – Pacific Cyber Safety, led to the adoption of the **Pacific-led Priorities Document on Technology-Facilitated Gender-Based Violence.** It called for strengthening legislation, policies, awareness, research and training across the region to address online abuse.[50] This was the first normative step explicitly framing TF VAWG within Pacific regional gender equality commitments, including the Pacific Leaders Gender Equality Declaration.[51] The document also emphasized reviewing national legal frameworks, closing legislative gaps and developing model provisions tailored to Pacific contexts, while prioritizing capacity-building for police, judicial actors and front-line services responding to gender-based violence. It identified regional coordination as critical, with recommendations to share resources, legal templates and advocacy strategies to respond collectively to TF VAWG.

CONCLUSION

This chapter highlights the increasing recognition of TF VAWG in global and regional normative frameworks, alongside its gradual integration into human rights and digital governance instruments. Several persistent gaps and challenges remain, however. These include:

1. **Fragmented definitions and scope:** The absence of a universally agreed definition of TF VAWG results in uneven interpretation and coverage across instruments, leading to inconsistent protections and obligations.
2. **Predominance of non-binding commitments:** Many global and regional agreements articulate principles but lack enforceable obligations, creating variability in national uptake and implementation.
3. **Uneven regional progress:** While some regions have embedded TF VAWG into binding frameworks, others rely on soft law or are still developing dedicated provisions, resulting in disparities in legal protections and enforcement.
4. **Lag between adoption and operationalization:** Recent commitments, both global and regional, often face long lead times before they are transposed into national laws and supported with resources for enforcement (see chapter 2).
5. **Limited alignment with technology governance**: Few normative frameworks integrate robust mechanisms to hold technology companies accountable or adapt to evolving harms linked to artificial intelligence, platform design and online business models.
6. **Data and monitoring gaps:** Across both the global and regional levels, limited and inconsistent data collection hinders the ability to track progress, assess impact and inform evidence-based policy responses.

Multistakeholder partnerships on technology-facilitated violence against women and girls

Collaborative efforts among multiple stakeholders to regulate online platforms and prevent TF VAWG are crucial to the safety and well-being of individuals, particularly women and marginalized groups, in digital spaces. Such initiatives are on the rise, involving governments, technology companies, civil society organizations, academia and international bodies. Below are some examples.

The Global Partnership for Action on Gender-Based Online Harassment and Abuse

The Global Partnership for Action on Gender-based Online Harassment and Abuse[52] brings together[53] partners committed to prioritizing, understanding, preventing and addressing the growing scourge of TF VAWG. It aims to create a comprehensive and multilevel strategy through intergovernmental work and its relationship with civil society and non-governmental organizations (NGOs). It is supported by a multistakeholder Advisory Group composed of victims-survivors, leaders and experts from civil society, research and academia, the private sector and international organizations.

Key elements

- Advances national, regional and multilateral policies and principles to address TF VAWG.
- Scales up programming and resources to respond to TF VAWG.
- Expands the supply and accessibility of reliable, comparable data.
- Collects best practices and shared principles to establish common experiences that harmonize prevention and response policies and programmes on TF VAWG.
- Promotes accountability for producing reliable and comparable data, at the national, regional and global levels, to understand the complexity of gender-based violence and establish public policies accordingly.

The Action Coalitions on Technology and Innovation for Gender Equality and on Gender-Based Violence under the Generation Equality

As part of the Generation Equality Forum held in 2021, the Action Coalition on Technology and Innovation for Gender Equality[54] identified TF VAWG as one of its four priority action areas. This generated more than 50 commitments from governments, private sector, CSOs, youth networks, United Nations Agencies and philanthropic organizations to develop policies, solutions and prevention initiatives against online and TF VAWG and discrimination, with dedicated targets to monitor and accelerate progress to meet the Agenda 2030 Goals. This work is complemented by the Action Coalition on Gender-Based Violence which aims at accelerating action towards the elimination of GBV against women and girls in all their diversity.

Key elements

- Aims to address TF VAWG, including online harassment, the non-consensual sharing of intimate images, and other forms of abuse that affect women and girls using technology.
- Advocates for stronger laws and policies to address TF VAWG and require online and tech companies to take responsibility for preventing and responding to it.
- Seeks to create a more inclusive digital ecosystem where women, girls and marginalized groups are equally represented in tech design and decision-making.

- Fosters multistakeholder partnerships, including through knowledge-sharing, exchanges of good practices, aligned efforts, shared resources and coordinated global approaches to leverage influence in ending TF VAWG.

Global Online Safety Regulators Network

Launched in November 2022, the Global Online Safety Regulators Network55 is a coalition of independent regulators – including the eSafety Commissioner (Australia), the Online Safety Commission (Fiji), Coimisiún na Meán (Ireland) and Ofcom (United Kingdom) – working together to address online harms through coordinated regulatory approaches. The network facilitates information-sharing, joint learning and the development of consistent standards to strengthen the accountability of online platforms, with particular attention to harms disproportionately impacting women and girls. It also engages with external observers, such as from civil society, academia, industry and multilateral bodies, to broaden collaboration and promote a rights-based approach to online safety.

Key elements

- Coordinates cross-border regulatory approaches to platform risk assessments and oversight, supporting coherent standards to address TF VAWG.
- Develops shared tools, such as the Online Safety Regulatory Index and collective position statements, to guide global practice.
- Provides an observer mechanism to include civil society, academia, international organizations and industry in knowledge-sharing and joint action.
- Strengthens capacities among regulators to hold platforms accountable for user safety, including in tackling image-based abuse and other forms of TF VAWG.

Photo: UN Women Sri Lanka/Jeewan Vithanage/Vimukthi Maduwantha-Raveendra Rohana

2

LEGISLATIVE MEASURES TO ADDRESS TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN AND GIRLS

Photo: UN Women Sri Lanka/Jeewan Vithanage/Vimukthi Maduwantha/Raveendra Rohana

National legal and policy responses to TF VAWG have developed unevenly but are expanding rapidly, often drawing on global and regional commitments while adapting to domestic legal traditions. In the absence of harmonized definitions or a standardized approach, countries have pursued a variety of pathways to legislate against TF VAWG, reflecting both the urgency of addressing new harms and the challenges of adapting existing frameworks. UN Women is working to address this gap through the production of a Supplement to the Handbook for Legislation on Violence against Women that is focused on TF VAWG specifically.

Broadly, three legislative approaches can be identified:

1. **The integration of TF VAWG within comprehensive VAWG legislation:** Some countries have expanded existing laws on violence against women and girls to explicitly cover digital and technology-facilitated forms of abuse. These comprehensive frameworks typically criminalize the most severe forms of VAWG, embed and implement preventive and protective measures, strengthen victim-survivor support (including through health, economic, psychosocial and legal services) and enforce appropriate penalties for perpetrators. They may facilitate multisectoral coordination across institutions and include mechanisms for monitoring implementation and collecting data.[56]
2. **Targeted legislative measures:** Some countries have adopted legislative measures specifically targeting select forms of TF VAWG, such as cyberstalking, digital harassment or the non-consensual dissemination of intimate images. This has entailed either amending existing laws originally focused on different forms of offline VAWG or adopting stand-alone laws solely addressing one or more forms of TF VAWG.

3. **Online safety and cyberlaws:** Many governments have used broader cybercrime or online safety frameworks to address forms of digital harm that overlap with TF VAWG. While not always explicitly framed through a gender lens, these laws often cover key offences, such as image-based abuse, cyberbullying or online exploitation. They may establish regulatory bodies to oversee compliance by technology companies and digital service providers.

Together, these approaches illustrate progress in recognizing and legislating against TF VAWG and the diversity of legal responses across jurisdictions. This chapter provides an overview of each approach, illustrated by examples from different countries. Please consult the **Global Database on VAWG** for additional examples of TF VAWG-related legislation.

1. INTEGRATING TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN AND GIRLS WITHIN COMPREHENSIVE LEGISLATION ON ENDING VIOLENCE

Olimpia Law, Argentina

In 2023, inspired by the pioneer Olimpia Law in Mexico,[57] Argentina enacted its own Olimpia Law.[58] This legislation amended the Integral Protection Law to Prevent, Punish and Eradicate Violence Against Women (Law 26.485),[59] adding "digital violence" across existing provisions to clarify their applicability in such cases. The law provides a broad definition of digital violence, covering multiple manifestations of "any conduct, action or omission against women based on their gender that is committed, instigated or aggravated, in part or in whole, with the assistance, use and/or appropriation of information and communication technologies, with the aim of causing physical, psychological, economic, sexual or moral harm, both in the private and public spheres, to them or their family group" (unofficial translation).

Key elements

- **Definition:** In addition to providing a broad definition of digital violence, the law specifies certain forms to which it can apply, including 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 and cyberattacks.
- **Protection for victims-survivors:** The law provides for a free and accessible multi-support telephone and digital helpline, and requests the compilation of service use data. It empowers victims-survivors to request the removal of harmful content and access legal and psychosocial support. It also allows them to seek protective measures, such as restraining orders, in response to online threats.
- **Penalties for offenders:** Offenders may face imprisonment of up to four years as well as financial penalties.
- **Responsibilities of digital service providers:** The law requires digital and online service providers to implement safeguards to prevent the dissemination of harmful content. They are required to remove content and cooperate in investigations of TF VAWG cases; non-compliance results in fines.
- **Preventative measures and education:** The legislation emphasizes public awareness and education to prevent digital violence. It mandates the Ministry of National Education to promote digital literacy programmes, encourage good practices in using ICT and facilitate the identification of digital violence. These initiatives are to be integrated into comprehensive sexuality education classes, other educational content and teacher training programmes.

Rose Leonel Law (Law No.13.772/2018), Brazil

In 2018, Brazil passed Law No. 13.722/2018.[60] It introduced significant amendments to both the Lei Maria da Penha (Law No. 11.340/2006)[61] and the Brazilian Penal Code (Decree-Law No. 2.848/1940)[62] aimed at addressing violations of women's privacy and TF VAWG. The law criminalized intimate image abuse and digital harassment and exploitation. It recognizes the role of digital platforms and online tools in perpetrating sexual violence, and acknowledges the increasing prevalence of TF VAWG as well as the severe harm that non-consensual image-sharing can cause. It applies to instances where deepfake technology is used to manipulate or fabricate intimate content.

Key elements

- **Definition:** The law includes non-consensual image-sharing in the definition of gender-based violence, recognizing it as a violation of privacy and personal dignity.
- **Penalties for offenders:** Penalties 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.
- **Protection for victims-survivors:** Comprehensive legal protections for victims-survivors of digital violence cover both criminal and civil legal actions as well as provisions for victim support and public awareness. These protections may include restraining orders, mandates to remove content from digital platforms and provisions helping victims-survivors to pursue legal action more effectively.
- **Responsibilities of digital service providers:** The law holds technology companies responsible for preventing the dissemination of non-consensual content, stipulating that they are expected to act against digital violence.

Law 15/2021, amending Galician Law 11/2007 on the prevention and comprehensive treatment of gender-based violence, Galicia, Spain

In 2021, the 2007 Galician Law on the Prevention and Treatment of Gender-Based Violence[63] (Ley 11/2007 de prevención y tratamiento integral de la violencia de género) added a provision on "digital violence, or online violence". This comprehensive law includes digital violence under Article 3 (h), which refers to "any act or conduct of gender-based violence committed, instigated or aggravated, in whole or in part, by the use of new information and communication technologies, such as the Internet, social media platforms, messaging and email systems, or geolocation services, with the aim of discriminating against, humiliating, blackmailing, harassing, or exercising control, dominance, or intrusion without consent into the victim's privacy" (unofficial translation).

Key elements

- **Definition:** The law adopts a broad definition of TF VAWG and explicitly applies regardless of whether the aggressor has or had a marital, romantic or similar emotional relationship with the victim in the present or past, or is related to the victim. The definition includes acts of digital violence against women committed by men in their family or social, professional or academic environment.
- **Prevention measures:** The law 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.
- **Research and knowledge production:** The law provides for a special research focus on TF VAWG, notably, to produce knowledge on

victims-survivors and perpetrators, the frequency and means through which such violence is committed, the impacts on victims-survivors and institutional responses.

- **Collaboration with the tech sector:** The law calls for the Government to promote collaboration with the main Internet intermediary platforms to establish flexible and urgent criteria and mechanisms for reporting and removing content related to digital gender-based violence.

The Domestic Violence Amendment Act of 2021, South Africa

South Africa's Domestic Violence Amendment Act of 2021[64] expands protections under the original Domestic Violence Act of 1998,[65] recognizing digital violence as a form of domestic abuse. The act acknowledges that domestic violence can occur through electronic communications, encompassing behaviours such as harassment, intimidation and emotional abuse conducted using digital platforms. Specifically, the 2021 amendments expand the legal framework to include coercive control, digital abuse, cyberharassment, online stalking and non-consensual image-sharing. These changes help protect victims-survivors under domestic violence laws.

Key elements

- **Protection for victims-survivors:** 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.
- **Responsibilities of digital service providers:** Courts can order digital platforms, including social media platforms, to take down abusive content.

2. TARGETED LEGISLATIVE MEASURES

Safe Space Act, The Philippines

The Safe Space Act, also known as the Republic Act No. 11313,[66] was passed in 2018 to address gender-based sexual harassment. The law includes "online" among the settings where sexual harassment can occur. It defines "gender-based online sexual harassment" as "an online conduct targeted at a particular person that causes or likely to cause another mental, emotional or psychological distress, and fear of personal safety, sexual harassment acts including unwanted sexual remarks and comments, threats, uploading or sharing of one's photos without consent, video and audio recordings, cyberstalking and online identity theft". A whole section of the law is dedicated to "gender-based online sexual harassment".

Key elements

- **Definition of TF VAWG acts and the use of an intersectional approach:** The law provides a list of acts in its definition of "gender-based online sexual harassment" to frame its application. Specifically, it lists "physical, psychological, and emotional threats, unwanted sexual misogynistic, transphobic, homophobic and sexist remarks and comments online whether publicly or through direct and private messages, […] cyberstalking and incessant messaging, uploading and sharing without the consent of the victim, any form of media that contains photos, voice, or video with sexual content, any unauthorized recording and sharing of any of the victim's photos, videos, or any information online, impersonating identities of victims online or posting lies about victims to harm their reputation, or filing, false abuse reports to online platforms to silence victims".
- **Implementing body:** The law clearly identifies the law enforcement body responsible for implementation (the Philippine National Police Anti-Cybercrime Group). 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 Center, is tasked with monitoring and penalization measures.

- **Penalties:** Provides penalties for individuals and juridical persons found guilty of digital violence, from fines to the revocation of licenses or franchises.

2025 Take It Down Act, United States

The Take It Down Act (S. 146), enacted as Public Law No: 119-12 on 19 May 2025,[67] is federal legislation in the United States aimed at combating non-consensual intimate visual depictions. These include both authentic photos and artificial intelligence-generated deepfake images that are published online with the intent to harass or harm. The law applies to "covered platforms", defined as public-facing websites or apps that host user-generated content. It requires them to remove such intimate images within 48 hours of receiving a valid takedown notice. Criminal and civil penalties are imposed on anyone who knowingly publishes or threatens to publish such imagery without consent. Violators may face fines, imprisonment (up to two years for adult victims, longer if minors are involved) and mandatory restitution. The legislation also requires platforms to create and publish a user-friendly takedown process within one year of enactment. At present, the Act explicitly excludes private, encrypted communications, such as on WhatsApp or Signal.

Key elements

- **Platform takedown obligations:** Covered platforms must establish a formal notice process requiring them to act within 48 hours of receiving a notice to remove content and attempt to delete all known copies.

- **Criminalization of non-consensual intimate imagery:** Publishing or threatening to publish intimate visual content (both real and artificial intelligence-generated) without consent, when intended to harm, is prohibited. The law applies to adults and minors, irrespective of their gender.

- **Enforcement and penalties:** Violators face restitution obligations and criminal sanctions, including imprisonment and fines.

- **Good-faith protections:** The law protects bona fide takedown requests and applies to hosting platforms.

Allow States and Victims to Fight Online Sex Trafficking Act/Stop Enabling Sex Traffickers Act (FOSTA-SESTA), 2018, United States

The FOSTA-SESTA legislative package amended the Communications Decency Act (Section 230)[68] to clarify that online platforms are not immune from liability under federal or state law for knowingly assisting, supporting or facilitating sex trafficking. It created new federal offences related to the promotion or facilitation of prostitution, including where such conduct involves reckless disregard that contributes to sex trafficking. The law enables both victims-survivors and state attorneys general to bring civil actions against entities that knowingly facilitate such crimes.

Key elements

- **Amendment to Section 230:** This narrows liability protections for interactive computer services, allowing prosecution and civil suits for the facilitation of sex trafficking.

- **New criminal offence (18 U.S.C. § 2421A):** This prohibits owning, managing or operating an interactive computer service with the intent to promote or facilitate prostitution, with enhanced penalties where sex trafficking is involved.

- **Civil remedy:** Victims-survivors gain the right to sue entities that violate § 2421A if they participated in sex trafficking.

- **State enforcement:** State attorneys general are authorized to bring civil actions in federal court against violators.
- **Relevance to TF VAWG:** The law represents a high-profile example of a national legal reform aimed at curbing the online facilitation of sexual exploitation, including trafficking, by imposing legal duties on platforms.

3. ONLINE SAFETY AND CYBERLAWS THAT ADDRESS TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN AND GIRLS

Online Safety Act, Australia

Australia's Online Safety Act 2021[69] aims to enhance online safety and protect individuals from online harms, including TF VAWG. While not uniquely focused on TF VAWG, it establishes a robust legal framework that places significant responsibility on digital platforms, social media companies and online service providers to manage and remove harmful content. The law empowers the eSafety Commissioner, Australia's national regulator, to address various forms of harmful digital conduct, such as cyberbullying, image-based abuse, cyberstalking and other forms of online harassment and exploitation. The eSafety Commissioner has the power to issue legally binding notices requiring platforms to take down content that constitutes online abuse, including some forms of TF VAWG.

Key elements

- **Support for victims-survivors:** The act provides support for victims-survivors, including access to legal remedies and the quick removal of harmful digital content. Dedicated services help individuals navigate the process of reporting and resolving online abuse. Victims-survivors can also request content removal, even if the perpetrator is not identified.
- **Responsibilities of digital service providers:** The act requires social media platforms to implement measures to mitigate the risk of cyberbullying and harassment. Hosting services must remove harmful content; search engines must delist or suppress links to harmful content upon the request of the eSafety Commissioner.
- **Penalties for non-compliance:** The act defines penalties for individuals and online platforms for their failure to comply with takedown notices.
- **Education and literacy:** An emphasis on public education on online safety includes programmes to prevent cyberbullying and image-based abuse. The act calls for raising awareness, teaching users to recognize and report harmful online behaviour, and providing resources for individuals to protect themselves from online harm.

Online Safety Act, Fiji

The Parliament of Fiji enacted the Online Safety Act 2018[70] to provide comprehensive protection, redress and compensation measures for victims-survivors of harmful online behaviour. While not explicitly focused on women and girls, the law provides a comprehensive legal framework to address a range of harmful online behaviours. It establishes the Online Safety Commission to support individuals exposed to harmful digital content. The commission provides services and resources to reduce harm and promote proactive online safety measures.

Key elements

- **Definition:** The act defines harmful online behaviour as any digital communication (e.g., messages, images, videos or social media content) that is abusive, offensive or threatening, causing harm to the recipient. This includes cyberbullying, cyberstalking and image-based abuse (non-consensual sharing of intimate images).
- **Protection and remedies for victims-survivors:** The act 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.

- **Penalties for offenders:** Criminal penalties for individuals who engage in harmful online behaviour include significant fines and imprisonment for cyberstalking, cyberbullying or the non-consensual sharing of intimate images. Specific penalties are prescribed for offences such as distributing harmful content or engaging in repeated harassment through digital means.
- **Responsibilities of online platforms and service providers:** The act requires online platforms and service providers to comply with removal orders and take appropriate action against harmful content and behaviours. If platforms fail to cooperate, they may face fines or other penalties. Digital platforms are held accountable for enabling or hosting harmful content.
- **Preventative measures and education:** Specific provisions aim to enhance public awareness of online safety and promote education on digital citizenship. The Government is tasked with supporting educational initiatives that teach individuals how to prevent online abuse and the implications of harmful digital behaviour.
- **Law enforcement:** The Online Safety Commission was established with the authority to act against online abuse, including by investigating alleged cases and providing victims-survivors with access to necessary support services.

CONCLUSION

This chapter shows the expansion in legislative responses to TF VAWG. Countries are adopting a range of approaches. These include integrating TF VAWG into comprehensive existing laws to end VAWG, adopting targeted legislative measures aimed at specific forms of TF VAWG, or passing broader cyber or online safety laws that include TF VAWG. Despite these developments, several ongoing gaps and challenges are evident. These include:

1. **Inconsistent legal coverage:** The absence of internationally agreed definition and standards leads to wide variation in how TF VAWG is defined and addressed, leaving some forms of abuse unregulated in certain jurisdictions.
2. **Limited adoption of comprehensive frameworks:** Many countries rely on narrow provisions, such as those specific to certain offences, rather than integrated laws to end VAWG that address the full continuum of online and offline violence.
3. **Gender-neutral approaches that overlook specific risks:** Cybercrime and online safety laws often lack a gendered lens. They thus fail to address the disproportionate impacts on and specific needs of women and girls.
4. **Weak enforcement and platform accountability:** Even where laws exist, enforcement is hindered by limited capacity, a lack of specialized training and an absence of binding obligations on technology companies.
5. **Privacy and rights concerns:** Some legislation to address TF VAWG contains measures to increase surveillance or target disinformation. This poses risks of overregulating online behaviour in ways that could silence dissent and infringe on privacy, anonymity and freedom of expression.
6. **Data and evidence gaps:** Limited disaggregated data on prevalence, prosecution and victim-survivor outcomes over time impedes assessments of legislative effectiveness and the ability to adapt laws to emerging forms of abuse.

3

MEASURES TO PREVENT TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN AND GIRLS

Photo: UN Women Africa

Preventing TF VAWG involves strategies aimed at stopping or reducing its incidence by addressing the drivers of VAWG, including gender inequality, harmful social norms and power imbalances that manifest both offline and online. Effective prevention seeks to both curb abusive behaviours and reshape the broader digital environment so that it is safer and more inclusive for women and girls. While evidence on what works to prevent TF VAWG is nascent, decades of work and research exist on effective prevention strategies for other forms of VAWG.[71] These findings informed the RESPECT Framework for Preventing Violence Against Women, widely used around the world.

Growing knowledge about TF VAWG, including on perpetration,[72] will continue to guide future work on prevention, including in understanding how to adapt tools such as RESPECT to prevent VAWG across the online-offline continuum. Current research is conducted by Equimundo in partnership with UN Women through a multicountry study on the perpetration of violence against women in online spaces. The research will provide insights on perpetrators of digital VAWG, their behaviours, tactics and motivations for the identification of effective prevention and response.

Emerging prevention efforts highlighted in this chapter include:

- **Advocacy and movement-building** that challenge harmful norms, raise the visibility of TF VAWG and mobilize collective action to secure safer digital spaces.

- **Awareness-raising campaigns** that inform the public, children, parents and educators about online risks and prevention strategies.
- **Educational programmes and digital literacy initiatives** that equip women, girls and young people with the knowledge and skills to navigate digital environments safely, while promoting critical understanding of online gender dynamics.
- **Safety-by-design and technological solutions** developed by civil society, governments and private sector actors to embed protection mechanisms into platforms, minimize harassment and empower users with greater control over digital interactions.

Together, such efforts reflect a growing recognition that preventing TF VAWG requires both confronting the structural inequalities that enable abuse and pursuing innovations in the design of digital tools, platforms and curricula to promote safer online engagement for all women and girls.

1. ADVOCACY AND MOVEMENT-BUILDING

Take Back the Tech, Global

Take Back the Tech[73] is a global, collaborative campaign developed by the Association for Progressive Communications to address TF VAWG through survivor-led, feminist approaches. It aims to enable women, girls and LGBTQI+ individuals to take control of digital spaces, enhance their digital skills, and use technology to combat violence, discrimination and inequality. The campaign blends digital security training, victim-survivor storytelling and advocacy as a model for feminist Internet governance. It works through local partners who adapt campaign actions and resources to different legal and cultural contexts. Its largest annual mobilization takes place during the international 16 Days of Activism Against Gender-Based Violence (25 November to 10 December).

Key elements

- **Digital security:** Equips participants with practical skills in encryption, secure communication, privacy and cybersecurity to protect themselves online.
- **Awareness-raising:** Raises awareness of online harassment, cyberstalking and abuse, promoting safer and more inclusive online spaces.
- **Digital literacy and access:** Addresses the digital divide, increases access to technology, and promotes the use of tech tools for social change, education and awareness.
- **Victim-survivor storytelling:** Creates platforms for victim-survivors to share experiences, build solidarity, and influence cultural and policy change.
- **Advocacy for policy changes:** Engages in lobbying and policy dialogue to protect women's rights in digital spaces and advances feminist Internet governance.
- **Community engagement:** Works with local and global communities to build networks for collective action and improve representation and safety for women and marginalized groups in technology.

TechHer NG, Nigeria

TechHer NG[74] is a Nigerian non-profit organization working to bridge the gender digital divide and address TF VAWG. Its programmes include digital safety clinics, online campaigns and capacity-building for women on privacy protection, identifying online abuse and safe technology use. TechHer NG applies an explicitly gender-focused lens, with particular attention to risks such as intimate image abuse, sextortion and harassment faced by women in online spaces.

Key elements

- **Digital safety clinics:** Community-based workshops provide hands-on training on online privacy, security settings and tactics to recognize digital abuse.
- **Campaigns and awareness-raising:** Public education initiatives use social media and offline outreach to increase women's digital literacy and resilience.
- **Gender-responsive design:** Programmes are tailored to the lived experiences and risks of Nigerian women and girls in online spaces.
- **Capacity-building:** Training supports activists, journalists and women leaders to use technology safely in advocacy and civic participation.

Clic Derechos, Argentina

Clic Derechos[75] is a national outreach programme developed by the National Secretariat for Children, Adolescents and Family under Argentina's Ministry of Social Development. It integrates digital rights education into school curricula and community initiatives, aiming to normalize discussions on TF VAWG and digital safety as part of youth education. The programme focuses on online threats that disproportionately affect women and girls, using tailored pedagogical strategies such as workshops on digital safety and partnerships with local organizations and schools to strengthen community participation.

Key elements

- **Youth-centred:** The programme recognizes the importance of engaging young people to prevent TF VAWG and provides them with tools and knowledge to navigate digital spaces safely and responsibly.
- **Educational approach:** Education for young people on digital citizenship promotes positive norms and respectful behaviours online and the safe use of technology.
- **Diverse pedagogy:** Combining multiple elements generates awareness of digital rights as part of broader cultural change
- **Advocacy and empowerment:** Advocacy encourages young people to become digital rights champions within their communities.

2. AWARENESS-RAISING CAMPAIGNS

BeSmartOnline! Programme, Malta

BeSmartOnline!'[76] is a collaborative effort by the Foundation for Social Welfare Services, the Directorate for Learning and Assessment Programmes, the Office of the Commissioner for Children and the Malta Police Force's Cybercrime Unit. The programme aims to address growing concerns about online safety, particularly for children and young people. It offers interactive workshops and sessions that teach students about online privacy, risks associated with sharing personal information, and how to recognize and avoid potential dangers such as cyberbullying and online harassment. It encourages community-wide efforts to prevent and promote safer digital behaviour. It also offers resources and tools to parents and educators, and empowers adults to guide young people in developing responsible online habits and recognizing the signs of TF VAWG.

Key elements

- **Youth-focused:** Raising awareness among younger populations helps to reduce risks in the medium and long term, and highlights the agency of women and children.
- **Support to victims-survivors:** The programme emphasizes access to assistance for victims-survivors while also working to hold perpetrators accountable.
- **Coordination:** Strengthened multistakeholder coordination brings together law enforcement, social services and other stakeholders.

3. EDUCATIONAL PROGRAMMES AND DIGITAL LITERACY

The Digital for Life Movement, Singapore

The Digital for Life Movement,[77] launched by the Government of Singapore in 2021, promotes digital inclusion, literacy and safety through partnerships with government agencies, educational institutions and technology companies. The initiative aims to respond to the digital needs of Singaporeans by providing tools and knowledge to navigate digital spaces safely. The Online Safety Digital Tools Resource Kit[78] compiles safety features from major platforms and offers step-by-step guidance on managing privacy, controlling interactions and reporting harmful content. These resources help users, particularly children, reduce exposure to online violence and exploitation and access reporting mechanisms.

Key elements

- **Survivor-focused resources:** Practical guides and educational materials empower users to manage online risks and take action against digital violence.
- **Multisectoral collaboration:** Engagement with government agencies, schools, community partners and technology companies promotes safer digital behaviour.
- **Digital for Life Fund:** The fund supports projects to advance digital inclusion and make safety and security central to Singapore's digital transformation.

The FTX: Safety Reboot, Global

The FTX: Safety Reboot[79] is a training curriculum developed by the Women's Rights Programme of the Association for Progressive Communications with a global network of trainers and activists. It equips women's and sexual rights defenders with skills to use digital technologies safely, creatively and strategically, embedding feminist principles and care into digital security training. The curriculum is community-driven and accessible, meeting participants where they are and valuing their existing knowledge. It includes six modules: creating safe online spaces, mobile safety, risk management, TF VAWG, feminist principles of the Internet and digital safety in storytelling. Materials are publicly available.

Key elements

- **Capacity-strengthening:** The programme builds activist and trainer capacity to address digital security comprehensively and holistically.
- **Accessible:** Practical, inclusive training is accessible regardless of prior expertise.
- **Co-creation:** Collaborative development with a global network has advanced a collective feminist approach to technology and security.

The Youth Guide to End Online Gender-Based Violence, Asia-Pacific

The Youth Guide to End Online Gender-Based Violence[80] is a toolkit developed by the 30 for 2030 Network, a youth and civil society leadership cohort in Asia-Pacific, with support from UN Women. Designed to be accessible and social media-friendly, the toolkit empowers young people, victims-survivors and civil society actors to take action against TF VAWG and build inclusive, gender-transformative digital spaces. The toolkit shares practical tips, highlights best practices from governments and non-governmental organizations (NGOs) globally, and provides recommendations for preventing TF VAWG and promoting safer online engagement. A second edition[81] offers important updates on bystander interventions and working with men and boys as allies to end TF VAWG.

Key elements

- **Youth empowerment:** The toolkit positions young people as key actors in shaping safe digital spaces, combining prevention and response strategies.
- **Contextual relevance:** Both regional and global practices illustrate how to adapt responses to different governance and cultural settings.
- **Multistakeholder approach:** Collaboration across governments, NGOs, tech companies and civil society supports comprehensive responses to TF VAWG.

Women's Services Network Technology Safety programme, Australia

The Women's Services Network Technology Safety[82] programme in Australia provides victims-survivors of domestic, family and sexual violence with tools, resources and training to address technology-facilitated abuse. The programme offers tailored guidance for victims-survivors on safeguarding devices, accounts and online presence, and equips front-line workers with the skills to support victims-survivors in navigating digital risks. It engages in policy advocacy to promote safety-by-design features in technology products and platforms.

Key elements

- **Victim-survivor resources:** Practical, accessible guides help victims-survivors in securing devices, managing privacy settings, detecting spyware and responding to online harassment.
- **Front-line worker training:** Specialized training helps domestic and family violence service providers identify and address technology-facilitated abuse.
- **Tech donation programme:** Partnerships with technology companies provide safe phones and devices to victims-survivors, reducing the risk of ongoing digital surveillance or abuse.
- **Safety-by-design advocacy:** Work with industry and government integrates victim-survivor safety considerations into technology design and policy.
- **Online resource library:** Up-to-date, publicly available resources cover common abuse tactics and digital safety strategies.

Empowering Schools to Improve Online Safety by Southwest Grid for Learning, United Kingdom

Southwest Grid for Learning[83] is a charity in the United Kingdom that aims at empowering schools to improve safety by providing a range of services and resources to promote safe and responsible technology use through education. It offers culturally sensitive and multilingual support to victims-survivors of online harm, including image-based abuse, harassment and sextortion. Services cater to diverse communities, making advice and reporting accessible regardless of language, cultural background or technical skill level.

Key elements

- **Educational resources:** Training and guidance help schools, parents and communities improve online safety and harm prevention.
- **Culturally sensitive support:** Tailored advice and resources for diverse cultural contexts improves accessibility in underserved communities.
- **Revenge Porn Helpline:** This confidential service supporting adult victims of non-consensual intimate image abuse is available in multiple languages.
- **Reporting harmful content:** A national reporting service assists individuals in flagging and removing harmful online material across platforms.

Photo: UN Women/Ploy Phutpheng

4. SAFETY-BY-DESIGN AND TECHNOLOGICAL SOLUTIONS FOR PREVENTION

Stop Non-Consensual Intimate Image Abuse (StopNCII.org), United Kingdom

StopNCII.org[84] is an initiative in the United Kingdom designed to support victims of non-consensual intimate image abuse. It provides a secure, effective, free, fast and anonymous tool to help victims-survivors stop their intimate images from being shared online, across participating platforms.

Key elements

- **Privacy-first hashing technology:** A digital fingerprint (hash) of each image generated locally ensures that the image never leaves the user's device. Images cannot be uploaded, stored or shared. Hashes are shared with participating platforms to block future uploads. Participating companies remove any matches that violate their intimate image abuse policy. StopNCII.org periodically scans for fingerprint matches.
- **Fast takedowns and future-proof prevention:** The initiative flags and removes existing content from partner websites, and prevents reuploads across platforms. This reduces the need for repeated victim-survivor reports, lowering retraumatization.
- **Support and resources:** Comprehensive support services include legal guidance, emotional support resources, and connections to digital safety and victim advocacy organizations. NGO partnerships and accessible support pathways strengthen victim-survivor trust.
- **Multiplatform and multistakeholder collaboration:** Working with social media platforms, technology companies and government bodies helps to create a united front against non-consensual intimate image abuse. The initiative partners with over 100 NGOs and helplines globally, enabling wider victim-survivor reach.

Tik Tok Safety Centre, China

TikTok[85] is a short-form video platform that has become a global cultural hub. It is especially popular among youth and marginalized communities. TikTok has developed a safety ecosystem grounded in user controls, proactive moderation, education and design-driven protections against technology-facilitated violence.

Key elements

- **Proactive content moderation:** Comment and keyword filters block offensive or unwanted content. The platform uses artificial intelligence-driven content moderation and nudges that prompt users to reconsider harmful posts before publishing.
- **Default privacy settings for youth:** "Private by default" settings for teens under 16 reduce grooming and coercion risks.
- **Regional and safety experts:** Regional safety teams, including specialists on gender-based violence, help to maintain safe user experiences on the platform.
- **Integrated safety and health hub:** An in-app Safety Hub offers mental health resources and partnerships with organizations active on ending gender-based violence.

Photo: UN Women Americas and the Caribbean

Bumble Dating App safety features, United States

Bumble[86] is a dating and social networking app known for its "women message first" approach and mission to create a safer, more respectful space for online dating. It applies safety-by-design principles through measures to prevent sexual harassment and image abuse as well as user empowerment.

Key elements

- **Proactive image blurring:** An artificial intelligence-powered feature detects and blurs explicit images.
- **Verified users:** Photo verification helps to reduce impersonation and fake accounts.
- **Proactive content moderation:** Proactive moderation limits hate speech, harassment and body shaming.
- **Diverse user controls:** These include incognito mode, location restrictions and profile visibility options.
- **Built-in safety centre:** An in-app Safety Centre provides trauma-informed resources and information on local helplines.

Building in safety-by-design

Safety-by-design approaches embed safeguards into platforms and products, and shift responsibility for online safety from users to technology companies.[87] For TF VAWG, this means integrating features that proactively prevent sexual harassment, abuse and exploitation.

Companies are increasingly adopting safety-by-design principles and creating tools that empower users to manage their digital interactions more securely. Three principles govern safety by design:[88]

1. Service provider responsibility to assess and address risks
2. Empowering users with safety and privacy controls
3. Upholding transparency and accountability

Applying these principles makes digital spaces safer and more resistant to abuse. UNFPA, the UK's Foreign Commonwealth and Development Office and Numun Fund, with the support of Australia's eSafety Commissioner, initiated the Safety Showcase,[89] a joint programme which aims to amplify innovators who share a passion for safe and ethical technology which places gender equality, inclusion and the lived experiences of women and girls at the heart of the design and development process.

BlockParty, United States

Block Party[90] is a third-party app that enhances user safety and privacy across major social media platforms. Initially focused on Twitter/X, it now supports over a dozen platforms, helping individuals, particularly those at risk of harassment, to take control of their digital presence.

Key elements

- **Option to block multiple abusive accounts at once (bulk blocking):** It also allows users to filter unwanted interactions.
- **User-enabled controls:** Batch deletion or hiding old posts reduces risks of doxing or targeted abuse.
- **Easily customizable control settings:** A one-click privacy setting adjustment covers multiple platforms.
- **Survivor-centred evidence preservation:** Tools help manage exposure to harassment while preserving evidence for reporting.

Perspective API by Jigsaw, United States

Perspective API,[91] developed by Google's Jigsaw, is an artificial intelligence tool that identifies toxic or harmful language in online discussions. It assists platforms and moderators in filtering abusive comments, thereby reducing risks of exposure. Some limitations in its efficacy include difficulties in detecting sarcasm and context as well as potential algorithmic bias.

Key elements

- **Scores harmful content:** The tool assigns toxicity scores to comments, flagging harassment, hate speech and discriminatory language.
- **Preventive content moderation:** Real-time content moderation occurs before posts go live.
- **Customizable thresholds:** Platforms can set customizable content moderation levels.
- **User feedback:** This encourages healthier online dialogue.

Photo: UN Women Africa

Photo: UN Women/Fahad Abdullah Kaizer

CONCLUSION

This chapter highlights the expanding range of prevention measures for TF VAWG, from awareness-raising campaigns and digital literacy programmes to safety-by-design innovations. While these initiatives demonstrate important progress, persistent gaps remain. These include:

1. **Burden on individuals:** Many initiatives still rely on women and girls to safeguard themselves online, without sufficiently addressing systemic drivers such as misogyny, gender inequality and discriminatory platform design.
2. **Weak links to offline prevention:** Few efforts draw on proven offline VAWG prevention strategies – such as norms change, transformative education and community mobilization – to address the root causes of digital violence against women and girls.
3. **Inconsistent adoption of safety-by-design:** While some companies have integrated proactive protections, uptake remains uneven across platforms. Protections are often voluntary rather than mandated.
4. **Limited reach and inclusion:** Prevention initiatives frequently focus on urban, digitally connected populations, leaving rural communities, those with low digital literacy and marginalized groups underserved.
5. **Fragmented and short-term:** Many interventions remain pilot-based or donor-dependent, with limited pathways to sustainability and scale.
6. **Insufficient funding for research to develop, test and evaluate interventions:** Shortfalls constrain implementation of the Technology-Facilitated Gender-Based Violence Shared Research Agenda and efforts to fill evidence gaps related to generative artificial intelligence.
7. **Need for partnerships:** More cross-sector collaboration is essential to generate stronger, more relevant evidence and responses.
8. **Insufficient evidence:** Few prevention measures are rigorously evaluated, hindering understanding of what works and limiting opportunities to strengthen policy and practice.

4

RESPONSE MECHANISMS

Photo: UN Women/Pathumporn Thongking

Increasing recognition of TF VAWG as a serious threat has made the development of effective response mechanisms a global priority. National governments, civil society and technology companies are investing in measures to support victims-survivors, improve accountability and strengthen institutional capacity.

Several trends are emerging:

- **Expansion of victim-survivor services:** Countries are beginning to integrate TF VAWG into existing psychosocial, legal, health and digital safety services. Although access remains uneven and often underresourced, trauma-informed and survivor-centred approaches are gaining traction as essential foundations of effective responses.
- **Growth of digital reporting and safety tools:** Platforms and independent developers are creating tools that enable victims-survivors to report abuse, remove harmful content and manage online risks more effectively. While promising, these tools are not yet universally accessible or consistently applied across platforms.

- **Specialized law enforcement and detection measures for minors:** Agencies are adopting new technologies to detect online child sexual exploitation and trafficking. But these responses often lack a gender lens. Girls are disproportionately targeted for grooming, coercion and sextortion.
- **Cross-border and multistakeholder collaboration:** The transnational nature of TF VAWG continues to challenge national responses, prompting greater international cooperation, data sharing and public-private partnerships.
- **Persistent gaps in reach and accountability:** Despite progress, many response mechanisms are pilots, fragmented or voluntary. Victims-survivors in marginalized or rural communities face significant barriers to access. Platform accountability often relies on self-regulation rather than binding obligations.

1. DIGITAL TOOLS FOR VICTIM-SURVIVOR SUPPORT AND SERVICE DELIVERY

The Cybercrime Prevention against Women and Children, India

The Cybercrime Prevention against Women and Children Scheme[92] in India is a government initiative to create a National Cybercrime Reporting Centre. The scheme seeks to prevent digital violence through research and development, training, awareness-raising and deterrence. It strives to educate the public about cyberthreats and safe online practices, and to establish accessible and efficient channels for reporting cybercrimes. It trains law enforcement agencies to handle cybercrime cases effectively. It also advocates for strengthening laws with stringent actions against perpetrators. The Government has implemented the scheme under the Nirbhaya Fund.[93]

Key elements

- **School-based programming:** School curricula have integrated cybercrime and cyberhygiene awareness components; awareness campaigns on types of cybercrimes and staying safe take place through a web portal and mobile apps.
- **Strengthening the capacities of the justice system:** Long-term courses and other avenues build the capacities of the central and state police forces, prosecutors and judicial officers on detection, investigation and forensic evidence.
- **Reporting mechanism:** The Online Cybercrime Reporting Portal provides a central repository of reported cases to inform an annual analytical report on cybercrimes.

Bloom, United Kingdom

Bloom[94] is an online platform created by Chayn, a civil society organization that supports victims-survivors of TF VAWG globally. Bloom provides support, resources and guidance on managing online abuse. It helps victims-survivors safely navigate legal and other technical steps to address TF VAWG while providing mental health resources and referrals to counselling and other services.

Key elements

- **Provides a safe space for victims-survivors:** All interactions are confidential and private so victims-survivors may seek support without fear of information becoming public
- **Applies a trauma-informed approach:** This includes acknowledging and responding to the impact of trauma on the user, using supportive and non-judgmental language.
- **Offers resources for digital safety:** Resources, including on how to secure accounts or phones and other privacy settings, help victims-survivors recover control of their online presence.
- **Supports victims-survivors to make plans to stay safe online:** Empowering victims-survivors with information helps them to reclaim their agency and make decisions, including on their digital security. Support helps victims-survivors

to think through safety plans and guides them in setting up a support network.

- **Provides information about direct service providers to support victims-survivors:** A global directory of support services helps victims-survivors access direct support as needed.

The National Centre for Digital Sexual Crime Response, Republic of Korea

The National Centre for Digital Sexual Crime Response[95] in the Republic of Korea provides round-the-clock support to victims-survivors. It is an initiative of the Women's Human Rights Institute of Korea, under the Ministry of Gender Equality and Family, and the National Centre for Digital Sexual Crime Response. First established in 2018,[96] the Centre was formally recognized as the central institution for responding to digital sexual crimes in 2025. It offers survivor-centred, law-based and technology-enabled action to report TF VAWG and extend support to victims-survivors. Teams provide counselling and help victims-survivors remove harmful and non-consensual images, whether real or deepfake. Artificial intelligence technology is used to proactively identify harmful content, resulting in the identification of more than 3 million cases of illegal content to date.

Key elements

- **Acts as a one-stop service centre for victims-survivors:** The Centre provides specialized support for victims of digital sexual violence, including referrals for medical, legal and investigative assistance.
- **Uses artificial intelligence to proactively flag and remove harmful content:** It monitors the (re)distribution of real and deepfake non-consensual images and provides victims-survivors with detailed takedown reports.
- **Facilitates referrals:** A national referral portal is available for both law enforcement and victim support agencies.

Pirth.org, Denmark and United States

Pirth.org is a global online resource hub to connect victims-survivors of online violence – including cyberbullying, doxing, exploitation, harassment and image-based abuse – to relevant, localized support. The platform provides tailored guidance on legal options, privacy checks and digital safety measures based on the user's location and needs. Victims-survivors have reported that they most appreciate its comprehensive, survivor-centred design and its ability to reduce the burden of navigating fragmented services. It covers over 50 countries across Africa, Asia, Europe, Latin America, Northern America and Oceania.

Key elements

- **Personalized resource matching:** The platform directs victims-survivors to country-specific legal information, helplines and safety tools based on their location and the type of abuse.
- **Comprehensive scope:** It addresses multiple forms of online sexual exploitation, including intimate image abuse, sextortion, grooming and related harms.
- **Victim-survivor-centred design:** It prioritizes confidentiality and accessibility, with guidance available in multiple languages and formats.
- **Global reach:** A verified database of services and partners in over 50 countries helps victims-survivors find support regardless of jurisdiction.
- **Evaluation insights:** Consolidating resources in one place reduces retraumatization; regular updates help keep information current and abreast of emerging threats.

Safety Net Project of the National Network to End Domestic Violence, United States

The Safety Net Project,[97] operated by the National Network to End Domestic Violence in the United States,[98] helps victims-survivors of domestic and sexual violence to navigate risks of technology-related abuse. It provides guidance on documenting incidents, compiling evidence and reporting abuse to platforms or authorities. It also trains service providers and advocates to assist victims-survivors in understanding their technology risks, enhancing their safety and exercising their rights in digital spaces.

Key elements

- **Documentation support:** The project offers step-by-step guidance for victims-survivors to collect and preserve evidence of online abuse, harassment or exploitation.
- **Reporting assistance:** It helps victims-survivors navigate reporting processes for platforms, law enforcement and regulatory bodies.
- **Training for advocates:** Building the capacity of front-line service providers helps them to recognize, respond to and prevent technology-facilitated abuse.
- **Technology safety resources:** A library compiles survivor-focused safety and privacy guides for different platforms and devices.

2. DEDICATED HELPLINES

The Cyber Harassment Helpline, Pakistan

The Cyber Harassment Helpline[99] was first set up by the Digital Rights Foundation in 2016. It was the first dedicated, toll-free helpline for victims-survivors of online harassment and violence in Pakistan. It provides free, safe and confidential services to victims-survivors who face or have faced harassment in digital spaces, including legal advice, digital security support, psychological counselling and referrals. The helpline actively works to reach marginalized groups, particularly minorities disproportionately targeted by online violence.

Key elements

- **Multiple channels:** Different communications channels (phone, email, social media) make the helpline widely accessible.
- **Intersectional approach:** Services in multiple languages respond to the needs of minorities who experience higher levels of online violence.
- **Confidential support and referrals:** Victims-survivors obtain confidential support and referrals to different services.
- **Safe space:** Victims-survivors gain a safe environment to share their experiences without judgment.

Speak Up Helpline, Egypt

The Speak Up Helpline[100] is an Egyptian feminist initiative providing confidential, survivor-centred support to individuals experiencing online blackmail, harassment and other forms of TF VAWG. It combines psychosocial and legal assistance with practical digital safety measures, addressing both the immediate harms and longer-term impacts of online abuse.

Key elements

- **Access to justice:** Legal guidance and referrals to trusted lawyers support victims-survivors in pursuing justice.
- **Mental health support:** Victims-survivors can reach trained psychologists offering confidential psychosocial support.
- **Content removal:** The helpline assists with content removal across major social media platforms, following up to ensure harmful material is fully taken down.
- **Survivor-centred approach:** A feminist and trauma-informed approach prioritizes victim-survivor autonomy, confidentiality and dignity.

Cyber Civil Rights Initiative, United States

The Cyber Civil Rights Initiative[101] is a non-profit organization based in the United States that is dedicated to combating non-consensual intimate images (still and video), sextortion and other forms of intimate image abuse. It operates a crisis helpline, provides safety planning and legal resources, and engages in policy advocacy to strengthen legal protections for victims-survivors. Its survivor-centred approach has informed state and federal legislative reforms, and its resources are accessed globally.

Key elements

- **Crisis helpline:** The initiative offers confidential support, safety planning and emotional assistance to victims-survivors of non-consensual pornography and related abuses.
- **Legal resource bank:** Guidance is available on relevant laws and reporting mechanisms in each state.
- **Policy advocacy:** The initiative has contributed to drafting and promoting non-consensual pornography laws across multiple states.
- **Public education:** An extensive library offers educational materials on image-based abuse and victim-survivor support strategies.

Netsafe, New Zealand

Netsafe is New Zealand's "approved agency" under the Harmful Digital Communications Act, mandated by the Ministry of Justice to receive and investigate complaints about harmful digital communications. Netsafe works to resolve cases through non-legal means and provides education and policy guidance on online safety. Its approach focuses on practical resolution, aiming to stop harmful behaviour and remove abusive content quickly, without requiring court interventions unless necessary.

Key elements

- **Complaint resolution:** Netsafe investigates harmful digital communication complaints and seeks to resolve them through advice, negotiation, mediation and persuasion.
- **Escalation to courts:** When cases cannot be resolved, it supports complainants in applying to the District Court, which may order removal or the disabling of harmful content.
- **Collaboration:** Strong relationships with domestic and international service providers improve enforcement and strengthen content removal mechanisms.
- **Education and policy:** Public guidance and resources on safe online practices contribute to prevention and cultural change around digital safety.

3. LAW ENFORCEMENT AND ACCESS TO JUSTICE

The High-Level Network on Gender Responsive Policing, guidance on addressing TF VAWG, global

The **High-level Network on Gender-Responsive Policing** was inaugurated in June 2024 during the Fourth United Nations Chiefs of Police Summit. It demonstrates strong Member State commitment to advancing gender-responsive policing, including strengthening institutions, preventing and responding to sexual and gender-based violence and ensuring perpetrator accountability.

Chaired by Chile, the Netherlands and Senegal, the network as of November 2025 comprises 21 Member States, with France leading Members in developing joint action on addressing TF VAWG. UN Women is Secretariat to the High-Level Network, and together with two of the Network's other Advisory Members, UNODC and UNDP, has developed guidance for police on preventing and responding to TF VAWG.[102]

Key elements

- **Enhanced response:** The global guidance helps police fully appreciate the severity of TF VAWG and provides them with examples of promising practices on institutional responses, including capacity-strengthening, prevention and fostering multi-stakeholder partnerships.
- **Improved reporting:** The guidance covers reporting entry points for TF VAWG that are survivor-centred and trauma-informed, and which consider the needs of all women and girls.

The Women and Children Cybercrime Protection Unit, Philippines

The Women and Children Cybercrime Protection Unit[103] is a specialized unit within the Philippine National Police's Anti-Cybercrime Group. Established to address TF VAWG, it investigates and prevents cases. The unit focuses on addressing online sexual exploitation of women and children, cyberstalking, sextortion, non-consensual sharing of intimate images, and online grooming and luring. It works closely with local partners, including NGOs and tech platforms, to identify perpetrators and protect victims-survivors.

Key elements

- **Access to support services:** The unit supports victims-survivors to access services, including psychological support.
- **Capacity-building:** Internal training and skills development help officers provide trauma-informed responses to TF VAWG.
- **Assistance in reporting cases of TF VAWG:** Support aids victims-survivors in filing cases under relevant laws.
- **Raises awareness:** Awareness campaigns take place on various forms of TF VAWG.

Violence Against Women and Girls Taskforce, National Centre for Violence and Public Protection, United Kingdom

The Violence Against Women and Girls Taskforce was set up by the National Centre for Violence and Public Protection in 2021 to support a coordinated policing response to VAWG. The taskforce has initiated several actions focused on technology-facilitated and online VAWG.[104]

Key elements

- **Adapted services:** The taskforce has rolled out new national online reporting and advice services for TF VAWG offences, including deepfakes and other image-based abuse, online stalking and sexual harassment, towards dismantling barriers to reporting.
- **Training:** The College of Policing developed an e-learning syllabus on digital investigation methods and tools aimed at front-line officers and staff. It includes a dedicated module on investigating technology-facilitated abuse and stalking.
- **Collaboration framework:** A tech working group was created with the VAWG and Rape and Serious Sexual Offences Taskforce as a platform for collaboration, making links to the Home Office, Crown Prosecution Services, Police Digital Service, other forces and the VAWG Taskforce. The working group provides a platform for police and partners to engage with tech suppliers.

Digital Platform for Victims of Cyberharassment, France

A digital platform run by the Ministry of the Interior in France provides 24/7 support to victims-survivors of cyberharassment,[105] allowing them to chat online with police officers specifically trained to respond to these cases. Victims-survivors can obtain support and are accompanied to file complaints in cases of insults and hate speech, hacking, doxing, non-consensual intimate image-sharing and digital domestic violence, among other forms of TF VAWG.

Key elements

- **Reporting assistance:** Victims-survivors can obtain help from a police officer to file a complaint, before being referred to appropriate legal services, local victim support partners, psychologists and legal information centres for comprehensive and personalized care.
- **Round-the-clock service provision:** The platform is free and accessible 24 hours a day, 7 days a week, from a computer, tablet or smartphone. It is also intended for witnesses, relatives of victims and professionals.
- **Trained service providers:** Approximately 50 police officers and gendarmes are trained and available to assist victims-survivors with necessary procedures, based on their respective cases.

The Cybercrime Online Reporting System, Mauritius

The Mauritian Cybercrime Online Reporting System[106] is a national online system that allows the public to report cybercrimes securely. It provides advice on recognizing and avoiding common cybercrimes on social media.

Key elements

- **Coordinated multisectoral action:** The system was set up through collaboration among various stakeholders, including the Ministry of Information Technology, Communication and Innovation; the Computer Emergency Response Team of Mauritius; the Attorney General's Office; the Cyber Crime Unit; the Information and Communication Technologies Authority and the Data Protection Office.
- **Awareness of digital safety:** The system provides education on different forms of digital violence and concrete tips on prevention and protection from cybercrimes on social media.

4. REPORTING MECHANISMS, PLATFORM ACCOUNTABILITY AND FACT-CHECKING

Instagram reporting mechanism, global

Instagram provides robust reporting tools to support users experiencing TF VAWG. These tools allow victims-survivors to report abusive content of online abuse (e.g., harassment, bullying, intimate image abuse), block or restrict harmful accounts, and access safety resources. Instagram focuses on user privacy, easy access to support and effective content moderation to create a safer online environment.

Key elements

- **Online reporting:** Users can report posts, comments, stories, direct messages and entire accounts for harassment, bullying and image-based abuse.
- **Confidentiality:** Anonymous reporting protects the identity of the victim-survivor.
- **Access to resources:** Resources on self-care, legal rights and emotional support include a safety centre with information on how to report abuse, access support and improve privacy settings.

YouTube flagging system, global

YouTube's flagging system[107] is core to its Community Guidelines and reporting mechanisms. It allows users to report content (e.g., videos, comments, live chats, channels and playlists) that violates policies, including hate speech, sexual harassment, threats, sexual content, privacy breaches and other harmful behaviour. Reports are processed using a combination of automated systems and human moderators, helping to identify harmful content and remove it quickly and efficiently. YouTube partners with governments and NGOs[108] to escalate serious violations, especially cases of online abuse and TF VAWG.

Key elements

- **Reporting menu:** This includes a structured reporting menu, artificial intelligence-enhanced content detection and a three-strike enforcement policy for repeat offenders.
- **Reporting transparency:** The system provides transparency on the status of reports and notifies offending content creators of strikes or takedowns with an option to appeal.
- **Proactive safety features:** Safety tools for channel owners include comment moderation filters, blocked word lists and tools to hide or ban abusive users. For content involving urgent or serious threats, YouTube's internal teams may work with law enforcement or crisis response channels.

Rappler disinformation and misinformation services, Philippines

Rappler is an online news site in the Philippines, founded in 2012. It is active in investigative journalism, explanatory journalism and civic engagement, and monitors governmental power, tracks corruption and examines democratic governance. Its mission includes combining journalism, community and technology to hold power to account. Rappler notably provides services on disinformation and misinformation.

Key elements

- **Fact-checking:** Rappler IQ is a fact-checking unit to monitor claims in the public sphere that might be false or misleading, verify them using primary sources and publish articles to correct facts.
- **Monitoring disinformation networks:** Rappler uses data analytics, social media monitoring and research to identify how disinformation spreads, including to detect fake accounts and observe patterns in the spread of false narratives.
- **Media literacy/public awareness:** Rappler promotes media literacy through fact-checking videos, webinars on fact-checking methodologies and media and information literacy, and community groups on social media platforms.
- **Technology tools and research:** Rappler embeds technology, data and research in its operations to map the spread of disinformation and analyse who is behind it and how it is shared.

Meta's Women's Safety Efforts

Meta, the parent company of social media platforms including Facebook, Instagram, and WhatsApp asserts that it recognizes the potential of the Internet and digital platforms for women's empowerment, when they are able to use it safely. Meta has established a Global Women's Safety Expert Group[109] that it convenes to inform the development of its policies, tools and resources.

Key elements

- **5 pillar approach to women's safety:** Meta bases its approach to women's safety on five essential pillars, including: Policies (including community standards), Tools for protecting yourself online, Help including a virtual help centre with step-by-step guidance to protect yourself against threats, Partnership including its Global Women's Safety Expert Advisors, and Feedback to gather user input to inform policies tools and resources.
- **Multisectoral expert input:** Meta's Women's Safety Expert Advisors represent diverse stakeholders, including academic, civil society organisations, human rights activists, representatives of multilateral organisations, and policymakers.

CONCLUSION

This chapter demonstrates the growing range of response mechanisms to TF VAWG, from victim-survivor support services and helplines to specialized law enforcement units and platform-based reporting tools. These are critical steps forward, but persistent gaps remain. These include:

1. **Barriers to access and inclusion:** Many mechanisms depend on Internet access, digital literacy and dominant language fluency, excluding rural and marginalized groups, and people and places with limited connectivity.
2. **Limited survivor-centred practice:** Services often lack adequate trauma-informed training and resources, undermining the safety, dignity and agency of victims-survivors.
3. **Fragmented systems:** Weak coordination between police, justice, health services and civil society leads to inconsistent referrals, delays and gaps in protection.
4. **Uneven platform accountability:** Company reporting tools vary widely in effectiveness, transparency and timeliness, with little external oversight.
5. **Low trust in authorities:** Victims-survivors may avoid reporting due to fear of retaliation, stigma or lack of confidence in the capacity of justice systems to respond.
6. **Insufficient cross-border cooperation:** Existing legal and operational frameworks have not kept up with the transnational nature of TF VAWG, leaving many cases unresolved.
7. **Lack of evidence on the impact of policies and regulations:** Many policies and regulations have been introduced in recent years, yet without evaluation to assess their impact and efficacy.

Photo: UN Women/Ploy Phutpheng

5

THE WAY FORWARD

Photo: UN Women/Ploy Phutpheng

The examples and trends documented in this Compendium show that while global, regional and national actors are increasingly recognizing and addressing TF VAWG, progress remains uneven, fragmented and often reactive. Legal and policy advances, prevention initiatives and response mechanisms have laid important groundwork. But significant gaps persist in definitions, enforcement, prevention, inclusion, coordination and accountability. To close these gaps and keep pace with a fast-evolving digital environment, collective action must be sustained, targeted and informed by the lived realities of victims-survivors and the emerging evidence base.

The following recommendations build on the findings from the Secretary-General's report[110] with a focus on multilateral action for strengthened national implementation based on lessons learned:

1. **Adopt a harmonized global definition and standards** The absence of a universally agreed-upon definition of TF VAWG leads to fragmented interpretations and inconsistent protections. Building consensus on a clear, inclusive, survivor-centred definition would reduce fragmentation, enable coherent cooperation, and provide a common basis for monitoring and accountability. Standards should be translated into legal and policy frameworks that are context and culturally specific to reflect the different harms and manifestations of TF VAWG in different regions and countries.

2. **Operationalize legal and policy framework**
Many global and regional commitments remain aspirational or lack enforcement. National laws must move beyond high-level statements to enact gender-responsive frameworks that cover the continuum of online and offline violence, backed by resources for enforcement, protection and prevention.

3. **Enhance technology company accountability**
Platforms remain central to shaping digital spaces, yet face few binding obligations. Enforceable safety-by-design standards, mandatory transparency reporting and independent audits should be introduced. Accountability frameworks must include clear penalties for non-compliance, alongside incentives to embed victim-survivor safety in platform design, moderation and business models.

4. **Strengthen prevention strategies**
Prevention remains underdeveloped relative to legislative and response measures. Governments, civil society and technology companies should scale up approaches that address the root causes of digital abuse – gender inequality, harmful norms and power imbalances – while adapting proven offline VAWG prevention models. Priorities include transformative, gender equality-focused education; awareness campaigns co-designed with youth and affected groups; investment in digital literacy and safety skills; and embedding safety-by-design principles into technology development. Prevention must reach rural and marginalized groups and those with low connectivity, not just digitally connected populations.

5. **Ensure survivor-centred and trauma-informed responses**
Responses must guarantee the rights, dignity and agency of victims-survivors. Governments, civil society organizations and service providers should ensure that services are widely accessible, confidential and culturally appropriate. Strengthened referral pathways linking the police, judicial system, healthcare, psychosocial support services and digital safety services are critical. Victims-survivors must be meaningfully engaged in shaping policies, programmes and platform tools. States should develop early warning indicators and systems to identify online violence that can escalate to offline violence.

6. **Invest in implementation capacity and support civil society**
Without capacity for implementation, laws and policies remain ineffective. Investment is needed to train law enforcement, the judiciary, regulators and service providers on survivor-centred approaches to responding to TF VAWG. Civil society and non-governmental organizations, often the first responders when State services are absent, must be adequately resourced to work on prevention, advocacy and direct service provision, recognizing their unique roles in bridging gaps.

7. **Prioritize the most vulnerable and at-risk groups**
Certain groups – including women in public life, feminist activists, LGBTQI+ individuals, girls, women with disabilities and those from minoritized communities – face disproportionate risks. Interventions must be tailored and accessible across languages, cultural contexts and connectivity levels. Responses to online child sexual exploitation must adopt a gender lens to recognize the distinct vulnerabilities of girls, while addressing the needs of boys and LGBTQI+ children.

8. **Advance cross-border cooperation and strengthen coordination and multistakeholder, cross-sectoral approaches**
TF VAWG is transnational. Stronger mechanisms for joint investigation, information-sharing and victim-survivor support across jurisdictions are essential. International cooperation should uphold human rights standards to balance safety, accountability and privacy. Fragmentation undermines impact. Governments, civil society organizations, tech companies, academia and international bodies should establish structured mechanisms for alignment, resource-sharing and joint strategies. Coordination should take

Photo: UN Women/Pathumporn Thongking

place nationally, regionally and globally. States, United Nations entities and other stakeholders should prioritise working together with technology companies to develop clear international standards and a framework for responding to TF VAWG.

9. **Expand research, monitoring and evidence-building**
   Data on TF VAWG remain inconsistent, fragmented and rarely disaggregated. Investment in regular, comparable, gender-sensitive data collection is needed to measure the prevalence, impact and effectiveness of interventions. Evaluations of laws, policies and programmes must feed back into practices and inform updates to this Compendium so it remains a living resource. Targeted support to advance the **Technology-Facilitated Gender-Based Violence Shared Research Agenda** would enable scholars and practitioners, particularly in low- and middle-income countries, to lead research that is relevant, responsive and capable of informing action.

Addressing TF VAWG is not solely a technological challenge. It is a societal imperative. Progress requires political will, coordinated multistakeholder action, and sustained investment in prevention, protection and accountability. The priorities outlined here form an interconnected roadmap; progress in one area reinforces progress in others. By acting on these priorities and adapting them as new evidence emerges, governments, civil society, technology companies and international actors can build safer, more equitable digital spaces for all women and girls, in all their diversity.

ENDNOTES

1 United Nations. 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. Available at **https://www.unwomen.org/sites/default/files/2024-10/a-79-500-sg-report-ending-violence-against-women-and-girls-2024-en.pdf**.

2 While this report uses TF VAWG, many different organizations and researchers use other terms to describe the same phenomenon, including technology-facilitated gender-based violence (TF GBV), ICT-facilitated violence, digital violence and cyberviolence, to name a few.

3 Harris, B., M. Dragiewicz and D. Woodlock. 2020. Technology, Domestic Violence Advocacy and the Sustainable Development Goals. In J. Blaustein, K. Fitz-Gibbon, N. W. Pino et al. (eds.), *The Emerald Handbook of Crime, Justice and Sustainable Development*. Emerald Publishing.

4 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.

5 See the glossary of additional terms related to TF VAWG in UN Women and World Health Organization. 2023. *Technology-Facilitated Violence Against Women: Taking stock of evidence and data collection*. Available at **https://www.unwomen.org/sites/default/files/2023-04/Technology-facilitated-violence-against-women-Taking-stock-of-evidence-and-data-collection-en.pdf**.

6 Economist Intelligence Unit. 2021. Measuring the Prevalence of Online Violence Against Women. The Economist Intelligence Unit.

7 Plan International and CNN As Equals. 2024. *Building Digital Resilience: Girls and Young Women Demand a Safer Digital Future.* Available at **https://plan-international.org/publications/building-digital-resilience/.**

8 Measuring the Prevalence of Online Violence Against Women.

9 Internet Watch Foundation. 2024. *Annual Data & Insights Report 2024*. Cambridge. Available at **https://www.iwf.org.uk/annual-data-insights-report-2024/data-and-insights/analysis-by-sex**.

10 Plan International and United Nations Children's Fund. 2020. *Free to Be Online? Girls' and Young Women's Experiences of Online Harassment*. London: Plan International.

11 National Center for Missing and Exploited Children. 2024. CyberTipline Report. Available at **https://www.missingkids.org/gethelpnow/cybertipline/cybertiplinedata**. *The Guardian*. 2025. FBI and NSPCC alarmed by 'shocking' rise in online sextortion of children. 9 August. Available at **https://www.theguardian.com/society/2025/aug/09/fbi-nspcc-alarmed-shocking-rise-online-sextortion-children**.

12 Council of Europe. 2022. No Space for Violence Against Women and Girls in the Digital World. Available at **https://www.coe.int/en/web/commissioner/-/no-space-for-violence-against-women-and-girls-in-the-digital-world.**

13 United Nations. 2022. Intensification of efforts to eliminate all forms of violence against women and girls: Report of the Secretary-General. A/77/302. Available at **https://www.unwomen.org/en/digital-library/publications/2022/08/intensification-of-efforts-to-eliminate-all-forms-of-violence-against-women-report-of-the-secretary-general-2022**

14 Cotter, A., and L. Savage. 2019. Gender-Based Violence and Unwanted Sexual Behaviour in Canada, 2018: Initial findings from the Survey of Safety

in Public and Private Spaces. Statistics Canada. Available at **https://www150.statcan.gc.ca/n1/pub/85-002-x/2019001/article/00017-eng.htm**.

15 Human Rights Council resolution 38/47, para. 28.

16 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, para. 8.

17 Incels, short for involuntarily celibate, are "a primarily online sub-culture community of men who forge a sense of identity around their perceived inability to form sexual or romantic relationships. The incel community operates almost exclusively online, providing an outlet for expressing misogynistic hostility, frustration and blame toward society for a perceived failure to include them". Speckhard et al., 2021, cited in Whittaker, J., W. Costello and A. Thomas. 2024. Predicting Harm Among Incels (Involuntary Celibates): The roles of mental health, ideological belief and social networking. Available at **https://www.researchgate.net/publication/378216114_Predicting_harm_among_incels_involuntary_celibates_the_roles_of_mental_health_ideological_belief_and_social_networking**.

18 UN Women. 2025. What Is the Manosphere and Why Should We Care? Available at **https://www.unwomen.org/en/articles/explainer/what-is-the-manosphere-and-why-should-we-care**.

19 Available at **https://www.un.org/womenwatch/daw/beijing/pdf/BDPfA E.pdf**.

20 UN Women. 2025. *Normative Advances on Technology-Facilitated Violence Against Women and Girls*. Available at **normative-advances-on-technology-facilitated-violence-against-women-and-girls-en.pdf**.

21 Mecanismo de Seguimiento de la Convención de Belém do Pará (n.d.). *Towards an Inter-American Model Law to Prevent, Punish, and Eradicate Gender-Based Digital Violence Against Women*. Available at **https://belemdopara.org/cim_mesecvi/gender-based-digital-violence-against-women/**.

22 Available at **https://www.un.org/womenwatch/daw/cedaw/**.

23 Available at **https://docs.un.org/en/CEDAW/C/GC/35**.

24 Available at **https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/CSW/57/CSW57-AgreedConclusions-A4-en.pdf**.

25 Available at **https://www.unwomen.org/sites/default/files/2023-03/CSW67_Agreed%20Conclusions_Advance%20Unedited%20Version_20%20March%202023.pdf**. See also UN Women on the sixty-seventh session of the Commission on the Statues of Women at **https://www.unwomen.org/en/csw/csw67-2023**.

26 Available at **https://digitallibrary.un.org/record/3999350?v=pdf**.

27 Available at **n2275964.pdf**.

28 Available at **https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf**.

29 Available at **https://docs.un.org/A/RES/79/152**.

30 Available at **https://digitallibrary.un.org/record/4071607?v=pdf**.

31 Available at **https://treaties.un.org/doc/Treaties/2024/12/20241224%2001-27%20PM/Ch_XVIII_16.pdf**.

32 Available at **https://documents.un.org/doc/undoc/gen/g18/214/82/pdf/g1821482.pdf**.

33 Available at **https://documents.un.org/doc/undoc/gen/g22/520/43/pdf/g2252043.pdf**.

34 Available at **https://documents.un.org/doc/undoc/gen/g23/146/09/pdf/g2314609.pdf**.

35 Available at **https://documents.un.org/doc/undoc/gen/g24/059/18/pdf/g2405918.pdf**.

36 Available at **https://documents.un.org/doc/undoc/ltd/g24/109/55/pdf/g2410955.pdf**.

37 Resolution on the Protection of Women Against Digital Violence in Africa (ACHPR/Res. 522 (LXXII) 2022). Available at **https://achpr.au.int**.

38 Available at **https://au.int/en/aucevawg**.

39 Available at **https://asean.org/wp-content/uploads/2021/01/The-Declaration-on-the-Elimination-of-Violence-Against-Women-and-Elimination-of-Violence-Against-Children-in-ASEAN.pdf**.

40 Available at **https://asean.org/wp-content/uploads/2018/01/48.-December-2017-ASEAN-RPA-on-EVAW-2nd-Reprint.pdf**.

41 ASEAN and UN Women. 2021. *Ending Violence against Women in ASEAN Member States: Mid-term review of the ASEAN Regional Plan of Action on the Elimination of Violence against Women*. Available at **https://www.spotlightinitiative.org/publications/ending-violence-against-women-asean-member-states-mid-term-review-asean-regional-plan#:~:text=Ending%20Violence%20against%20Women%20in,Violence%20against%20Women%20(RPA%20on**.

42 Available at **https://www.coe.int/en/web/istanbul-convention/about-the-convention**.

43 Available at **https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147**.

44 Available at **https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065**.

45 European Parliamentary Research Service. 2024. Cyberviolence Against Women in the EU. Briefing. Available at **https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/767146/EPRS_BRI(2024)767146_EN.pdf**.

46 Available at **https://eur-lex.europa.eu/eli/dir/2024/1385/oj/eng**.

47 Available at **https://belemdopara.org/wp-content/uploads/2021/11/texto-de-la-convencion-INGLES.pdf**.

48 Mecanismo de Seguimiento de la Convención de Belém do Pará y ONU Mujeres. 2022. Informe. Ciberviolencia y Ciberacoso contra las mujeres y niñas en el marco de la Convención Belém Do Pará. Available at **https://lac.unwomen.org/es/digital-library/publications/2022/04/ciberviolencia-y-ciberacoso-contra-las-mujeres-y-ninas-en-el-marco-de-la-convencion-belem-do-para**.

49 Mecanismo de Seguimiento de la Convención de Belém do Pará. 2024. MESECVI Launches Regional Consultations on the Model Law to Combat Technology-Facilitated Violence Against Women in Argentina, Colombia, and Panama. Available at **https://belemdopara.org/wp-content/uploads/2024/12/Press-Release-Consultations-Model-Law-Nov-2024.pdf**.

50 Available at **https://hrsd.spc.int/sites/default/files/2024-07/TFGBV%20Priorities%20Document-Pacific%20symposium_v2.1.pdf**.

51 Pacific Community. 2024. A First Pacific-Led Priorities Document to Better Address Online Abuse. Blog post. Available at **https://www.spc.int/updates/blog/blog-post/2024/04/a-first-pacific-led-priorities-document-to-better-address-online**.

52 See more at **https://2021-2025.state.gov/2023-roadmap-for-the-global-partnership-for-action-on-gender-based-online-harassment-and-abuse/**.

53 Australia, Canada, Chile, Denmark, Finland, France, Iceland, Japan, Kenya, Mexico, New Zealand, Republic of Korea, Spain, Sweden, the United Kingdom and the United States.

54 See more at **https://forum.generationequality.org/action-coalitions**.

55 See more at **https://www.esafety.gov.au/about-us/consultation-cooperation/international-engagement/the-global-online-safety-regulators-network**.

56 UN Women. 2012. *Handbook for Legislation on Violence Against Women*. Available at **https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/Library/Publications/2012/12/UNW_Legislation-Handbook%20pdf.pdf**.

57 The Olimpia Law (named after Olimpia Coral Melo, who was a victim of intimate image abuse in 2011) has been important in recognizing the gravity of TF VAWG at the national level. This has led to reform of

the penal code to incorporate new types of crime. It laid foundations for the coordination and implementation of actions to prevent, respond and eliminate TF VAWG in Mexico. These include the criminalization of sextortion, threats, cyberharassment, sexual harassment and non-consensual image-sharing. See more at **https://www.alignplatform.org/sites/default/files/2024-10/align-mexico-digitalsexualviolence-execsummary-eng-digital.pdf**.

[58] Available at **https://www.argentina.gob.ar/noticias/ley-olimpia-el-gobierno-promulgo-la-legislacion-que-incorpora-la-violencia-digital-como-una**.

[59] Available at **https://www.boletinoficial.gob.ar/detalleAviso/primera/296572/20231023?utm**.

[60] Available at **http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13772.htm**.

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

[62] Available at **https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm**.

[63] Available at **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**.

[64] Available at **https://www.justice.gov.za/legislation/acts/2021-014.pdf**.

[65] Available at **https://www.justice.gov.za/legislation/acts/1998-116.pdf**.

[66] Available at **https://lawphil.net/statutes/repacts/ra2019/ra_11313_2019.html#:~:text=These%20establishments%20are%20obliged%20to,immediately%20coordinate%20with%20local%20authorities.**

[67] Available at **https://www.congress.gov/bill/119th-congress/senate-bill/146**.

[68] Available at **https://www.congress.gov/bill/115th-congress/house-bill/1865**.

[69] Available at **https://www.legislation.gov.au/C2021A00076/latest/text**.

[70] Available at **https://laws.gov.fj/Acts/DisplayAct/2462#**.

[71] For more information about evidence-based prevention practices, see **https://ww2preventvawg.org/evidence-hub**.

[72] See, for example, Harris, B., R. Fiolet, C. Brown et al. 2023. Technology-Facilitated Abuse in Relationships. University of Melbourne. Available at **https://socialequity.unimelb.edu.au/__data/assets/pdf_file/0006/4587594/Technology-Facilitated-Abuse-in-Relationships-Report-2023.pdf**.

[73] See more at **https://www.takebackthetech.net/**.

[74] See more at **https://techherng.com/**.

[75] See more at **https://www.argentina.gob.ar/noticias/clic-derechos-avanza-la-implementacion-del-programa-para-prevenir-el-grooming-en-todo-el**.

[76] See more at **https://www.besmartonline.info/**.

[77] See more at **https://www.digitalforlife.gov.sg/**.

[78] See more at **https://www.digitalforlife.gov.sg/learn/resources/all-resources/tools-and-resources-for-managing-your-own-safety-online**.

[79] Available at **https://www.apc.org/en/pubs/feminist-tech-exchange-safety-reboot-curriculum**.

[80] Available at **https://asiapacific.unwomen.org/en/digital-library/publications/2023/12/youth-guide-to-end-online-gender-based-violence**.

[81] Available at **https://asiapacific.unwomen.org/en/partnerships/30-for-2030/toolkit-second-edition-of-the-youth-guide-to-end-online-gender-based-violence**.

[82] See more at **https://techsafety.org.au/**.

[83] See more at **https://swgfl.org.uk/**.

[84] See more at **https://stopncii.org/**.

[85] See more at **https://www.tiktok.com/community-guidelines/en/overview**.

[86] See more at **https://bumble.com/en/the-buzz/safety**.

[87] See more at **https://www.esafety.gov.au/industry/safety-by-design**.

[88] See more at **https://www.esafety.gov.au/industry/safety-by-design#safety-by-design-principles; https://www.futurelearn.com/info/courses/safety-by-design/0/steps/349752**.

[89] See more at **https://www.tfgbvsafetyshowcase.org/**.

[90] See more at **https://www.blockpartyapp.com/faqs/how-does-block-party-work**.

[91] See more at **https://perspectiveapi.com/**.

[92] See more at **https://www.mha.gov.in/en/division_of_mha/cyber-and-information-security-cis-division/Details-about-CCPWC-CybercrimePrevention-against-Women-and-Children-Scheme**.

[93] The Nirbhaya Fund was established to provide financial support to initiatives aimed at enhancing the safety and security of women across India. Its primary focus is to support projects and programmes that address violence against women, including by assisting victims-survivors. See more at **https://pib.gov.in/PressReleasePage.aspx?PRID=2110881#:~:text=A%20number%20of%20schemes/%20projects,headed%20by%20women%20police%20officers**.

[94] See more at **https://bloom.chayn.co/auth/register**.

[95] See more at **https://www.stop.or.kr/streamdocs/view/sd;streamdocsId=11sqOJYAymSKsNXA3v-zLtYSVBqHmJgaNb7ASvZSzais**.

[96] See more at **https://d4u.stop.or.kr/**.

[97] See more at **https://www.techsafety.org/**.

[98] See more at **https://nnedv.org/**.

[99] See more at **https://digitalrightsfoundation.pk/cyber-harassment-helpline/**.

[100] See more at **https://speakupeg.com/helpline/**.

[101] See more at **https://cybercivilrights.org/**.

[102] UNODC, UNDP and UN Women. Guidance for Police on addressing technology-facilitated gender-based violence, *forthcoming*.

[103] See more at **https://www.facebook.com/PNPACGWCCPU/?locale=ka_GE&utm_source=chatgpt.com**.

[104] Herdale, G., K. Duddin and O. Jurasz. 2025. Landscape Review: Policing Technology-Facilitated and Online Violence Against Women and Girls. Milton Keynes, UK: Centre for Protecting Women Online. Available at **https://oro.open.ac.uk/104074/8/104074VOR.pdf**.

[105] See more at **https://www.masecurite.interieur.gouv.fr/fr/demarches-en-ligne/plateforme-signalement-cyberharcelement**.

[106] See more at **https://maucors.govmu.org/maucors/**.

[107] See more at **https://transparencyreport.google.com/youtube-policy/removals?hl=en**.

[108] See more at **https://support.google.com/youtube/answer/7554338?hl=en**.

[109] See more at **https://www.meta.com/safety/communities/women/?srsltid=AfmBOoppRGun-Dxuy9bx5VloQwBKmtoaIJaZUKNPNT-o4J2cf-p9emd9SV#partners**.

[110] United Nations. 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. Available at **https://www.unwomen.org/sites/default/files/2024-10/a-79-500-sg-report-ending-violence-against-women-and-girls-2024-en.pdf**.

UN WOMEN EXISTS TO ADVANCE WOMEN'S RIGHTS, GENDER EQUALITY AND THE EMPOWERMENT OF ALL WOMEN AND GIRLS.

As the lead UN entity on gender equality and secretariat of the UN Commission on the Status of Women, we shift laws, institutions, social behaviours and services to close the gender gap and build an equal world for all women and girls. Our partnerships with governments, women's movements and the private sector coupled with our coordination of the broader United Nations translate progress into lasting changes. We make strides forward for women and girls in four areas: leadership, economic empowerment, freedom from violence, and women, peace and security as well as humanitarian action.

UN Women keeps the rights of women and girls at the centre of global progress – always, everywhere. Because gender equality is not just what we do. It is who we are.

UN WOMEN

FOR ALL WOMEN AND GIRLS

220 East 42nd Street
New York, New York 10017, USA

unwomen.org
facebook.com/unwomen
x.com/un_women
youtube.com/unwomen
flickr.com/unwomen