

Technology Facilitated Violence against Women and Girls: International and regional human rights standards, gaps and opportunities

June 2026



Lawyers
for Justice
in Libya



Centre for
Protecting
Women Online



The Open
University

Acknowledgements

This publication is the result of a collaboration between Lawyers for Justice in Libya (LFJL) and the Centre for Protecting Women Online (CPWO). The research has been funded by The Open University's Open Societal Challenges strategic funding dedicated to research development at CPWO.

About Lawyers for Justice in Libya (LFJL)

LFJL is a people centred, Libyan and international human rights non-governmental organisation seeking transformative justice to create long term systemic change. LFJL challenges the underlying social, cultural, economic, ecological, and political conditions that give rise to injustice, corruption, and violence in Libya. Its work focuses on movement building to strengthen civil society; addressing daily injustices and institutional reform; advancing accountability for serious international crimes and human rights violations; and promoting equality and non-discrimination as the foundation of a just society. LFJL has been working on TFVAWG for the past six years, including documenting the scale of online violence against women in Libya in a 2021 report¹ as well as filing the first ever complaint involving TFVAWG with the Committee on the Elimination of Discrimination against Women (CEDAW Committee).²

About the Centre for Protecting Women Online (CPWO)

CPWO is a cross-disciplinary unit dedicated to advancing women's online safety through research and cross-disciplinary collaborations. The Centre has five inter-woven work streams: law and policy; human behaviour; the future of responsible tech; ethical and responsible tech/AI; and policing. CPWO is funded by Research England's Expanding Excellence in England (E3) grant. CPWO is focused on advancing understanding of and addressing challenges to women's safety online, working collaboratively across disciplines and sectors to inform research, organisational practice and government decision making. CPWO aims to reduce online harms suffered by women and girls, promote prosocial behaviours online and help build better and more responsible tech and software.

The following people produced this report:

Research project leads: Juergen Schurr (LFJL) and Professor Olga Jurasz (CPWO)

Research lead: Marwa Ben Abderrazek (LFJL)

Design and illustrations: Areej Bader (LFJL)

¹ LFJL, [We Will Not Be Silenced: Online Violence Against Women in Libya, 9 March 2021](#).

² LFJL, Press release: [Libya has failed to comply with its CEDAW obligations in a case of severe online violence against Noura Aljerbi, 2 July 2024](#).

Table of Content

List of Abbreviations	4
1. Context	5
2. Summary of findings	6
2.1 TFVAWG as a human rights violation	6
2.2 TFVAWG and State obligations	9
2.3 Responsibilities of tech companies and social media platforms	11
3. Gaps and areas for further development.	13
4. Advocacy and Litigation	16
Annex Table 1. Global normative development of TFVAWG	18
Annex Table 2. Regional normative development of TFVAWG	21

List of Abbreviations

AU (African Union)
ACHPR (African Commission on Human and Peoples' Rights)
AU-CEVAWG (African Union Convention on Ending Violence Against Women and Girls)
AI (Artificial intelligence)
CEDAW (Committee on the Elimination of Discrimination against Women)
CRC (Committee on the Rights of the Child)
CSW (Commission on the Status of Women)
ECtHR (European Court of Human Rights)
EU (European Union)
GREVIO (Group of Experts on Action against Violence against Women and Domestic Violence)
HRC (Human Rights Council)
ICT (Information and Communication Technology)
IACHR (Inter-American Commission on Human Rights)
ICCPR (International Covenant on Civil and Political Rights)
SRRWA (Special Rapporteur on the Rights of Women in Africa)
TFVAWG (Technology Facilitated Violence Against Women and Girls)
UN Women (United Nations Entity for Gender Equality and the Empowerment of Women)
UNGA (United Nations General Assembly)
WPS (Women, Peace and Security)

1. Context

Technology facilitated violence against women and girls (TFVAWG) is a fast -growing serious human rights issue affecting women and girls globally. Digital tools, including social media, artificial intelligence (AI), tracking and monitoring technologies, enable new and rapidly evolving forms of abuse that outpace relevant legal frameworks. How international and regional human rights mechanisms respond to this challenge matters, as they can provide guidance to states to comply with their human rights obligations, and serve to equip advocates and litigators with the tools to better prevent and protect against TFVAWG.

LFJL and the CPWO carried out research into how key international³ and regional⁴ human rights mechanisms have approached TFVAWG as a human rights violation, including violence occurring online, through digital platforms and through other technology mediated means. This also included examining specific state obligations to respect, protect and fulfil human rights in the context of TFVAWG, as well as responsibilities of corporate actors such as technology companies and social media platforms. The research examines standard setting instruments, including resolutions, general comments, concluding observations, thematic reports and related guidance.

The research is designed to identify existing normative approaches, gaps and opportunities for future strategic engagement with relevant mechanisms, including through advocacy and standard setting strategic litigation to influence policy, shape human rights guidance and strengthen legal protections. It informs the development of an agenda and background paper for a virtual expert roundtable. The research and outcomes of the roundtable discussions will subsequently support the development of a practical handbook on TFVAWG for advocates and litigators.

³ With a focus on key UN bodies, including Special Rapporteurs and UN treaty bodies.

⁴ This includes the relevant bodies from the African, European, and Inter-American human rights systems.



2. Summary of findings

2.1 TFVAWG as a human rights violation

A range of United Nations (UN) and regional human rights mechanisms have adopted instruments directly or indirectly dealing with TFVAWG. In the absence of a treaty on TFVAWG, these provide important guidance on how to approach TFVAWG as a human rights violation. They articulate binding state obligations under existing human rights treaties as interpreted by treaty bodies, and non-binding but potentially significant recommendations from intergovernmental bodies and expert mechanisms which help clarify the corresponding obligations of states and responsibilities for companies and platforms.

Overall, this report reflects the current state of play in the development of international and supranational standards of TFVAWG, indicating an emerging understanding of TFVAWG not only as individualised online abuse, but as part of a continuum of gender-based violence⁵. This includes recognition of harms such as online harassment, cyberstalking, doxing, non-consensual intimate image (NCII) sharing, sextortion, gendered disinformation, AI generated deepfakes and technology enabled surveillance. These developments indicate that TFVAWG affects not only women's safety and dignity, but also their rights to equality and non-discrimination, privacy, freedom of expression, access to information, political participation, education and public life.

CEDAW General Recommendation No. 35 (2017), for example, clearly states that TFVAWG constitutes gender-based violence (GBV)⁶ and as such amounts to discrimination and constitutes a **violation of human rights**. The UN General Assembly similarly affirmed that TFVAWG violates, and impairs women's and girls' **"full enjoyment of, all human rights"** while the Secretary-General in his 2024 report on TFVAWG highlighted that TFVAWG is a serious and growing form of gender-based violence (GBV)⁷. The 2018 thematic report on TFVAWG by the then Special Rapporteur on Violence against Women and Girls (2018 SRVWG Report) sets out how international human rights law applies in the context of TFVAWG⁸.

The UN Convention against Cybercrime⁹, adopted in December 2024, is the first global treaty on cybercrime and electronic evidence, but it is not a treaty on violence against women and girls or a comprehensive human rights instrument. It does not use TFVAWG as a standalone term yet

5 CEDAW para.6 expressly refers to a "continuum" including technology mediated settings and para.20 covers violence in online/digital environment.

6 Committee on the Elimination of Discrimination against Women (CEDAW Committee), General Recommendation No.35 on gender-based violence against women, updating general recommendation No.19, (CEDAW Committee, General Recommendation No.35), paras. 6, 20.

7 UN Secretary General, Intensification of efforts to eliminate all forms of violence against women and girls: [technology-facilitated violence against women and girls, 8 October 2024, A/79/500, \(UN SG 2024 Report\)](#).

8 Human Rights Council, [Report of the Special Rapporteur on Violence against Women, Its Causes and Consequences on Online Violence against Women and Girls from a Human Rights Perspective, A/HRC/C/38/47, 18 June 2018, \(SRVWG 2018 Report\)](#) paras. 50 – 61.

9 United Nations Convention against Cybercrime; [Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes, 24 December 2024, C.N.196.2025](#). The Convention is open for signature until 31 December 2026, and enters into force once at least 40 states have ratified it. At the time of writing (June 2026), 77 states had signed, and three states had ratified the Convention.

several provisions are directly relevant to TFVAWG¹⁰. For example, it addresses wider forms of TFVAWG, including online harassment, cyber stalking, doxing, digitally enabled coercive control, gendered disinformation, platform amplified misogynistic abuse or AI generated sexualised deepfakes.

A further development is the growing framing of TFVAWG within conflict, cybersecurity and women, peace and security frameworks. **The 2026 CEDAW Addendum to General Recommendation No.30 on women in conflict prevention, conflict and post conflict situations in relation to the Women Peace and Security (WPS)** Agenda situates cyberspace as a site of gender-based violence before, during and after conflict. This includes online harassment, disinformation, deepfakes, sextortion, cyber trafficking and targeted attacks against women political leaders, human rights defenders, LGBTQI+ defenders, journalists and peacebuilders. This recognises that TFVAWG should not be treated solely as a digital safety or criminal justice issue, but also as a conflict, democratic participation and peace and security concern¹¹.

At the regional level, although **the African Union Convention on Ending Violence Against Women and Girls**¹², does not expressly use the term TFVAWG, it provides a human right basis for addressing such violence. In its Preamble, the Convention recognises that violence against women and girls occurs in “public and private spheres and in cyber space” and affirms that such violence constitutes a violation of women’s and girls’ human rights and fundamental freedoms. This is reinforced by Article 2, which recognises the right of every woman and girl to live free from all forms of violence as indivisible from and interdependent with other human rights and fundamental freedoms¹³. However the Convention’s treatment of TFVAWG has been criticised as conceptually and operationally limited¹⁴.

The African Commission on Human and Peoples’ Rights (ACHPR) has been more progressive and adopted several standard setting instruments on violence against women, including TFVAWG. Its resolution on the Protection of Women against Digital Violence in Africa (ACHPR/Res.522 (LXXII)2022) builds on the Protocol to the African Charter on Human and Peoples’ Rights on the Rights of Women in Africa (Maputo Protocol) and extends protections into the digital space, urging states to recognise digital violence as forms of GBV¹⁵.

10 Several international human rights organisations have criticised the Convention, see [Human Rights Watch, warning that the Convention extends beyond cyber-dependent crimes and enables broad electronic surveillance and evidence sharing without adequate safeguards](#), Access Now [criticised the Convention for overbroad criminalisation and insufficient safeguards](#), while Article 19 warned that [cybercrime legislation can enable human rights violations under the guise of national security](#).

11 CEDAW Committee, Addendum to General Recommendation No.30 on women in conflict prevention, conflict and post conflict situations in relation to the Women, Peace and Security Agenda, 2026, paras. 4,9,27, 83-86: see also Human Rights Council, Report of the Special Rapporteur on violence against women and girls, its causes and consequences, Sex based Violence against women and girls: new frontiers and emerging issues, A/HRC/59/47, 1 May 2025, paras.53-55.

12 [African Union Convention on Ending Violence Against Women and Girls, February 2025](#).

13 African Union Convention on Ending Violence Against Women and Girls, Preamble, arts 1(k), 2 and 3(a).

14 For example, of this critique, see #PauseforPurpose, Form Over Substance: A Critique of the Protection against Tech- Facilitated Violence in the African Union Convention on Ending Violence against Women and Girls (Briefing paper, 2025), sections 2.1-2.2; Article 19, African Union Convention on Ending Violence Against Women and Girls (2025), 14-15. These sources criticise the Convention for failing to expressly define or name TFVAWG, for treating cyberspace largely as a location where violence occurs rather than recognising technology as a tool that can be used to commit, assist, aggravate or amplify TFVAWG and for failing to provide practical guidance on how to prevent and protect against it.

15 African Commission on Human and Peoples’ Rights (ACHPR), [Resolution on the Protection of Women Against Digital Violence in Africa - ACHPR/Res. 522 \(LXXII\) 2022, 11 August 2022](#).

“The African Commission **calls on States to Review/adopt legislation** that aims at **combating all forms of digital violence**, and **expanding the definition of gender-based violence to include digital violence against women including:**

**cyber-harassment,
cyberstalking
sexist hate speech**

amongst other ICT-related violations”

In the Inter-American human rights system, the **Belém do Pará Convention** remains the cornerstone of the regional response to violence against women and has significantly influenced national legal reforms across Latin America¹⁶. It is also the only human rights treaty specifically on violence against women with an individual complaint mechanism, empowering the Inter-American Commission on Human Rights (IACHR) and Inter-American Court of Human Rights to receive cases¹⁷. The Convention affirms that all **“women have the right to a life free from violence both in physical spaces and in digital environments.”** The Inter-American Model Law¹⁸ to Prevent, Punish and Eradicate Gender Based Digital Violence against Women was developed by the Committee of Experts of the Follow-up Mechanism to the Belém do Pará Convention (MESECVI). Adopted in 2025, it is designed as a regional legislative tool to guide states in adapting their domestic laws to address technology-facilitated and digital forms of GBV. The Model Law defines gender based digital violence against women, sets out states’ preventive, protective, investigative, punitive and reparative duties and establishes detailed obligations for internet intermediaries within a co-regulatory framework. This positions the Inter- American system as a regional leader in translating a general VAW treaty into concrete, operational standards on TFVAWG.

16 Cinar, E. (2021). Main Features of the Inter- American Convention on Violence Against Women. Available at [OSEI.O](https://www.osei.io).

17 Bettinger -Lopez, C. (2018). Violence Against Women: Normative Developments in the Inter-American Human Rights System. In R.Manjoo & J. Jones (eds.), [The Legal Protection of Women from Violence: Normative Gaps in International Law](https://www.routledge.com/The-Legal-Protection-of-Women-from-Violence-Normative-Gaps-in-International-Law/book/9781138380000). Routledge.

18 Follow up Mechanism to the Belem do Para convention (MESECVI), InterAmerican Model Law to Prevent, Punish and Eradicate Gender Based Digital Violence against Women, OEA/Ser.L/II/7.10, MESECVI/CEVI/doc.299/25, 10 December 2025, ch I, art 2.

The Inter-American Commission of Women's report on online gender-based violence against women and girls (2022) also makes clear that TFVAWG is a continuation of offline violence, rooted in systemic gender inequality and discrimination¹⁹.

In Europe, the Council of Europe Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO), in charge of monitoring the implementation of the Convention on preventing and combating violence against women and domestic violence (Istanbul Convention), increasingly examines not only VAW, but also specifically TFVAWG, and how states are preventing and combating TFVAWG. In 2021, it adopted General Recommendation No.1²⁰, making clear that the Istanbul Convention applies to digital violence against women, and providing detailed guidance on states' obligations to prevent, protect and prosecute TFVAWG²¹. This guidance was reinforced in March 2026, when the Committee of Ministers adopted Recommendation CM/Rec(2026)2 on Accountability for TFVAWG²², the first regional legal standard dedicated specifically to this issue, which builds on GREVIO's General Recommendation No.1 by treating TFVAWG not merely as a regulatory gap but as a human rights harm requiring redress across criminal, civil and administrative law including through obligations on technology companies to adopt a safety by design approach.

2.2 TFVAWG and State obligations

The research examined a range of state obligations when it comes to TFVAWG, as set out comprehensively in the UN General Assembly's resolution (A/RES/79/152) on the Intensification of efforts to prevent and eliminate all forms of violence against women girls: the digital environment (December 2024). The General Assembly urges states to **“take appropriate measures for the prevention of all forms of violence....against women online and through digital technologies, and to protect them in online spaces and considering adopting laws, policies and practices that protect them from defamation and hate speech while also respecting their human rights and fundamental freedoms”**²³.

The UN Secretary-General highlights in his 2024 report that states should adopt laws that **“address technology – facilitated violence against women and girls”**²⁴. The 2018 SRVWG report makes clear, and sets out, that states “have a human rights obligation to ensure that both State and non-State agents refrain from engaging in any act of discrimination or violence against women.” This includes the obligation to prevent, protect, prosecute, punish and repair harm as the result of TFVAWG, as well as due diligence obligations to “prevent, investigate and punish acts of

19 Inter-American Commission of Women (CIM), [Online gender-based violence against women and girls – Guide of basic concepts, 2022](#).

20 GREVIO General Recommendation No. 1 on [the digital dimension of violence against women \(2021\)](#).

21 Council of Europe, [Group of Experts on Action against Violence against Women and Domestic Violence \(GREVIO\)](#). GREVIO is also part of the “Platform of Independent Expert Mechanisms on Discrimination and Violence against Women (EDVAW Platform)”, which, in November 2022, issued [a thematic paper on the digital dimension of violence against women providing a\) an overview of the nature, scale and impacts of TF-VAWG; b\) approaches taken by the EDVAW mechanisms; c\) identifying some practices and challenges reported by the mechanisms; and d\) proposing some common action to be taken by the EDVAW Platform](#).

22 Council of Europe Committee of Ministers, [Recommendation CM/Rec\(2026\)2 of the Committee of Ministers to member States on accountability for technology facilitated violence against women and girls](#), adopted 4 March 2026.

23 UN General Assembly, Resolution 79/152, [Intensification of efforts to prevent and eliminate all forms of violence against women and girls: the digital environment](#), (UNGA Resolution 79/152), 19 December 2024, para. 5(x).

24 UN SG 2024 Report, para.31.

violence against women committed by private companies... in line with Article 2 (e) of the CEDAW convention”²⁵.

Broader due diligence obligations as highlighted for example by the Human Rights Committee in its General Comment No.31 in relation to obligations under the ICCPR, and the Committee against Torture in its General Comment No.2 in relation to obligations under the UN CAT, may also be invoked under certain circumstances in the context of TFVAWG. At the regional level, the Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) issued General Recommendation No.1 on the digital dimension of violence against women in October 2021, with a list of measures State Parties to the Istanbul Convention should take to abide by their obligations under the Convention to prevent, protect against, and prosecute TFVAWG²⁶.

To fulfil their obligation to protect against TFVAWG, CEDAW General Recommendation No.35 recommends that states provide police training, protective measures and mechanisms for reporting digital abuse. According to CEDAW, this obligation to protect extends to acts or omissions by committed private individuals or corporations if the state fails to act with due diligence.

CEDAW General Recommendation No.35 also calls on states to provide access to reparation for victims and to **“establish a system to regularly collect, analyse and publish statistical data on the number of complaints about all forms of gender-based violence against women, including technology-mediated violence”**²⁷. UN General Assembly Resolution 79/152 urges states **“to take immediate and effective action to prevent and eliminate all forms of violence against women and girls that occur through or are amplified by the use of technology, and to support and protect all victims and survivors by”**, amongst other things, providing **“for effective access to appropriate remedies and reparations for victims and survivors”**²⁸.

25 SRVWG 2018 Report, para.62.

26 Council of Europe, GREVIO issued [General Recommendation No.1 on the digital dimension of violence against women, 20 October 2021, paras.49 – 57](#).

27 CEDAW Committee, General Recommendation No.35, para.34 (b).

28 UNGA Resolution 79/152, para. 6 (a).

2.3 Responsibilities of tech companies and social media platforms

Some instruments also explicitly set out the responsibility of private companies, including technology companies and social media platforms, to ensure respect for human rights. For example, CEDAW General Recommendation No.35 encourages

“the creation or strengthening of self-regulatory mechanisms by media organizations, including online or social media organizations...addressing gender-based violence against women that takes place through their services and platforms”²⁹.

The SRVWG’s 2018 report highlights that “Internet intermediaries” have specific human rights responsibilities that have yet to be fully addressed under the international human rights framework³⁰.

The UN General Assembly Resolution 79/152 (December 2024) sets out a range of measures tech companies, internet providers and social media platforms should take to prevent TFVAWG, including: **“mainstreaming a gender perspective in the conceptualisation, development and implementation of digital technologies and related policies; and promoting the participation of women in order to address violence and discrimination against women and girls in digital contexts, inter alia by encouraging digital technology companies, including Internet service providers, and digital platforms to respect standards and implement effective, inclusive, transparent and accessible reporting mechanisms”³¹.**

The Committee on the Rights of the Child (CRC) also frames business actors as having responsibilities to prevent and remedy harms to children in the digital environment, including through rights due diligence, safety by design, privacy by design and effective remedies³².



²⁹ CEDAW Committee, General Recommendation No.35, para.30 (d) (i).

³⁰ SRVWG 2018 Report, para.71.

³¹ UNGA Resolution 79/152, para. 5 (u) – (w).

³² Committee on the Rights of the Child, General Comment No. 25 (2021) on children’s rights in relation to digital environment, CRC/C/GC/25 (2 March 2021), paras. 36-39 (business sector responsibilities and child rights due diligence/impact assessments), para.42(de-sign-related measures) and para.49 (remedies).

Across the instruments reviewed, the responsibilities of technology companies and social media platforms are increasingly recognised but remain unevenly developed. Relevant standards refer to self-regulation by online and social media organisations³³, human rights due diligence³⁴, child rights due diligence³⁵, safety by design and privacy by design³⁶, accessible reporting mechanisms³⁷, transparency³⁸, content moderation³⁹, remedies⁴⁰ and cooperation with states and civil society⁴¹. The CRC provides one of the most detailed frameworks on business responsibilities in the digital environment⁴², requiring states to ensure that business prevents their networks and online services from being used in ways that cause or contribute to violations or abuses of children's rights⁴³ and that children, parents and caregivers have access to prompt and effective remedies⁴⁴.

In the EU context, the EU Digital Services Act⁴⁵ requires platforms to address illegal and harmful content, including NCII, it also introduces obligations for online platforms concerning illegal content, transparency⁴⁶, while the EU AI Act⁴⁷ introduces transparency obligations in relation to AI-generated or manipulated content, including deepfakes⁴⁸. In the African system, African Commission on Human and Peoples' Rights (ACHPR) Resolution 630; which is principally concerned with information integrity and fact checking; calls for stronger corporate accountability, human rights due diligence, transparency and monitoring of technology companies⁴⁹, particularly in high-risk contexts such as elections and conflict. In the Inter American system, the Mechanism to Follow up on the Implementation of the Belem do Para Convention (MESECVI) finalised in December 2025, an Inter-American Model Law on the Prevention, Punishment and Eradication of TFVAWG which sets out regulatory obligations for technology service providers alongside state due diligence obligations under Article 7 of the convention⁵⁰.

33 CEDAW Committee, General Recommendation No. 35, para. 30 (d) (i).

34 UN Human Rights Council, Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework, A/HRC/17/31, 21 March 2011, Principles 11, 15 and 17; Committee on the Rights of the Child, General Comment No. 25 on children's rights in relation to the digital environment, CRC/C/GC/25, 2 March 2021, paras. 35-38.

35 Committee on the Rights of the Child, General Comment No. 25, paras. 35-38.

36 Committee on the Rights of the Child, General Comment No. 25 paras. 38 and 77.

37 UN General Assembly, Resolution 79/152, Intensification of efforts to prevent and eliminate all forms of violence against women and girls: the digital environment, A/RES/79/152, 19 December 2024, para. 5 (u) - (w); Committee on the Rights of the Child, General Comment No. 25, para. 48.

38 Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single Market For digital Services and amending Directive 2000/31/EC, OJ L 277/1, 27 October 2022, arts. 15, 24, 27, 39 and 42; Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, OJL, 12 July 2024, art. 50.

39 Committee on the Rights of the Child, General Comment No. 25 para 56; Regulation (EU) 2022/2065, arts. 14-17 and 34-35.

40 Committee on the Rights of the Child, General Comment No. 25, paras. 36 and 48; UN Human Rights Council, Guiding Principles on Business and Human Rights, A/HRC/17/31, Principles 22, 25 and 29.

41 UN General Assembly Resolution 79/152, paras. 5 (u) - (w); CEDAW Committee, General Recommendation No. 35, para. 35 (a).

42 Committee on the Rights of the Child, General Comment No. 25, paras. 35-38 and 48.

43 Committee on the Rights of the Child, General Comment No. 25, para. 48.

44 Committee on the Rights of the Child, General Comment No. 25 para. 48.

45 [The Digital Services Act](#).

46 Regulation (EU) 2022/2065, arts. 16, 22, 24, 27, 34, 35 and 38.

47 European Commission. (2026). [AI Act. Shaping Europe's Digital Future](#).

48 Regulation (EU) 2024/1689, art. 50.

49 African Commission on Human and People's Rights, Resolution on developing Guidelines to assist states to monitor technology companies in respect of their duty to maintain information integrity through independent fact checking, ACHPR/Res. 630 (LXXXII), 2025.

50 Follow up Mechanism to the Belem do Para convention (MESECVI), InterAmerican Model Law to Prevent, Punish and Eradicate Gender Based Digital Violence against Women, OEA/Ser.L/II/7.10, MESECVI/CEVI/doc.299/25, 10 December 2025, ch I, art. 2.

A further issue is the **linguistic fragmentation**, and, in some cases, the **outdated terminologies** employed across international and regional frameworks, as reflected in the interchangeable use of terms such as “online violence”, “cyberviolence”, “ICT-related violence”, “technology facilitated gender-based violence”, “technology facilitated violence” and “technology facilitated violence against women and girls”. The absence of a unified legal definition risks diluting conceptual precision and weakens enforcement. Moreover, terms such as “cyberbullying” or “cyber harassment” may understate the severity and gendered nature of harms, while also more technical terms such as “ICT-related violence” reflect an outdated understanding of digital environments and does not capture the emerging forms of abuse, including AI enabled abuse.

Existing standards are only beginning to address the specific risks posed by emerging technologies particularly AI⁵². However, reviewed standards still provide important guidance on how states and companies should prevent, investigate, regulate and remedy these harms particularly where they involve AI-enabled abuse, algorithmic amplification, cross border perpetrators or technology companies⁵³.

Further guidance is needed on **AI-enabled TFVAWG**, including transparency around AI generated or manipulated content⁵⁴, risk assessment and human rights safeguards in the use of artificial intelligence⁵⁵, safety by design and privacy by design approaches⁵⁶, platform accountability and due diligence obligations⁵⁷, and remedies for victims and survivors of AI enabled TFVAWG.

Similarly, there is some acknowledgment of the important **role of tech companies and social media platforms in preventing and protecting against TFVAWG**, yet their responsibilities and corresponding mechanisms for accountability - remain somewhat vague, are voluntary and lack enforcement structures. For example, while the AU-CEVAWG requires states to engage social media platforms and the advertising industry in prevention efforts (Article 10), it frames this as a state obligation rather than imposing direct responsibilities on technology companies themselves leaving this gap in direct corporate accountability. This gap is particularly important in the African context, where human rights and feminists civil society organisations have cautioned that the AU-CEVAWG’s reference to cyberspace does not yet amount to a comprehensive TFVAWG framework and should be strengthened through explicit definitions, enforceable state obligations, platform

52 Human Rights Council, Report of the Special Rapporteur on Violence against Women, its causes and Consequences, Sex based violence against women and girls: new frontiers and emerging issues, A/HRC/59/47, 1 May 2025, para.53. See also CEDAW Committee, Addendum to General Recommendation No.30 on women in conflict prevention, conflict, and post conflict situations in relation to the Women, Peace and Security Agenda 2026, paras.4 and 9.

53 Human Rights Council, Report of the Special Rapporteur on Violence against Women, Its causes, and Consequences on Online Violence against Women and girls from a Human Rights perspective, A/HRC/38/47, 18 June 2018, paras. 71-76; CEDAW Committee, Addendum to General Recommendation No.30 on women in conflict prevention, conflict, and post conflict situations in relation to the Women, Peace and Security Agenda 2026, paras. 83-86.

54 Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence.

55 UN General Assembly Resolution 79/152, Intensification of efforts to prevent and eliminate all forms of violence against women and girls: the digital environment, 19 December 2024.

56 Committee on the Rights of the Child, General Comment No.25 on Children’s rights in relation to the digital environment, CRC/C/GC/25, 2 March, paras.38 and 77.

57 CEDAW committee, Addendum To general Recommendation No.30, 2026, para.83; African Commission on Human and People’s Rights, ACHPR/Res.630(LXXXII), 2025.

accountability standards, algorithmic transparency, content moderation duties, survivor centred remedies and cross border cooperation⁵⁸.

In contrast, the Inter-American system illustrates a more progressive approach: the December 2025 Inter-American Model Law⁵⁹ on Gender Digital Violence against Women goes further by establishing detailed obligations for internet intermediaries within a co-regulatory framework. Implementation and enforcement remain untested given how recently the Model Law was adopted. This approach was reinforced in Europe as of March 2026, when the Council of Europe Committee of Ministers adopted Recommendation CM/Rec (2026) 2 on accountability for TFVAWG, the first dedicated international instrument on the issue, explicitly addressing platform responsibility⁶⁰. The recommendation calls on member states to adopt clear and transparent regulatory measures requiring online platforms to prevent and combat TFVAWG, including through effective content moderation, adequately trained human moderators, gender sensitive and transparent AI systems, timely removal of unlawful content, evidence preservation, accessible redress mechanism and measures to mitigate algorithmic amplification of misogynistic or violent content.

Existing instruments as examined by the research also seem to provide only minimal guidance on how to address **the extraterritorial nature of TFVAWG** (for example, from multinational platforms) and how states can enforce obligations (and be held responsible) when platforms are based abroad.

Overall, common with human rights obligations generally, domestication and implementation of relevant standards including, where they exist, explicit TFVAWG obligations, remain a challenge as many countries lack the infrastructure, technical expertise or political will to address TFVAWG.

58 Initiative for Strategic Litigation in Africa, ["Form Over Substance: A Critique of the Protection against Tech- Facilitated Violence in the African Union Convention on Ending Violence against Women and Girls"](#).

59 Follow up Mechanism to the Belem do Para convention (MESECVI), InterAmerican Model Law to Prevent, Punish and Eradicate Gender Based Digital Violence against Women, OEA/Ser.L/II/7.10, MESECVI/CEVI/doc.299/25, 10 December 2025.

60 Council of Europe Committee of Ministers, [Recommendation CM/Rec\(2026\)2 of the Committee of Ministers to member states on accountability for technology facilitated violence against women and girls](#), adopted 4 March 2026.

4. Advocacy and Litigation

Building on the above, there are a range of opportunities for TFVAWG advocates and litigators to further develop and strengthen the international and regional frameworks, and to contribute to their implementation domestically. This includes:

- Engaging with relevant UN treaty bodies to develop specific guidance (through General Comments, thematic reports, reporting guidelines for states around TFVAWG) on how TFVAWG is linked to their respective mandates and identify concrete, practical, measures states should take to uphold their obligations to prevent, protect against and repair TFVAWG harm where it occurs.
- Filing TFVAWG cases to UN treaty bodies identifying the link between TFVAWG and relevant mandates and highlighting systemic challenges at domestic level to prevent, protect against and remedy TFVAWG.
- Working with progressive regional mandates, such as the ACHPR, and particularly its Special Rapporteur on Freedom of Expression and Access to Information in Africa and the Commissioner on Violence against Women, in the development of Guidelines around TFVAWG designed to “enable states Parties to effectively monitor the platforms’ performance in order to inform of the efforts to advance information integrity online, including the role of independent fact-checking in the African context”⁶¹.

⁶¹ ACHPR, Resolution on developing Guidelines to assist states to monitor technology companies in respect of their duty to maintain information integrity through independent fact checking, ACHPR/Res.630 (LXXXII), 2025.



- Exploring benefits and potential of a UN special procedure mandate on TFVAWG to consolidate findings, issue thematic reports, engage states and identify pathways for accountability and redress.
- Mainstreaming TFVAWG as a cross-cutting issue across all human rights advocacy and reporting mechanisms including UN treaty bodies, body reviews, the Universal Periodic Review and Special Procedures.
- Working towards binding international standards on technology companies and social media platforms, building on relevant HRC and UNGA resolutions and on regional guidance such as the Council of Europe Committee of Ministers Recommendations CM/Rec(2026)2 on accountability for TFVAWG and CM/Rec(2026)1 on equality and AI. This could include obligations to conduct impact assessments, disclose moderation policies and compensation (and other forms of reparation) for victims of platform enabled harm.
- Advocating for specific guidance on AI- enabled TFVAWG, including deepfakes, synthetic intimate images, algorithmic amplification, recommender systems, targeted gendered disinformation, cyberstalking and technology enabled surveillance.
- Working in national / regional coalitions on the implementation and domestication of existing regional instruments, including, in particular, in the African, European and Inter-American contexts. This could include the development of relevant model legislation or legislative provisions (taking inspiration from the Model Law on Gender Digital Violence against Women in the Inter-American system), capacity building to strengthen institutional frameworks as well as engagements with tech companies and social media platforms. At the European Union level, member states have until June 2027 to implement the 2024 EU Directive on combating violence against women and domestic violence into domestic legislation. This could provide an opportunity to develop relevant material (guidelines, model legislation etc) to support domestic implementation.

Annex Table 1. Global normative development of TFVAWG

Year	Normative instruments	Key elements related to TF VAWG
2011	UN Guiding Principles on Business and Human Rights	- Establishes corporate responsibility to respect human rights globally and across all business activities. - Requires companies to conduct human rights due diligence. - Due diligence must address VAWG, including TF VAWG, within corporate value chains.
2016	Human Rights Council (HRC) Resolution A/HRC/RES/32/13	Notes that human rights should apply in online spaces as they do offline, reinforcing the importance of safeguarding rights of women and girls against gender-based violence in all areas of life.
2017	Committee on the Elimination of Discrimination against Women (CEDAW) General Recommendation No. 35	- Recognises gender-based violence against women as a continuum that includes digital, online, and tech-mediated violence. - Expands states' obligations to include technology-mediated settings in prevention and response efforts. - Recommends data collection and international cooperation to combat digital forms of violence against women.
2018	Report of the Special Rapporteur on Violence against Women, Its Causes and Consequences on online violence against women and girls from a human rights perspective A/HRC/38/47	- First UN thematic report on VAWG in digital contexts; defines cyber harassment, doxing, sextortion, and non-consensual image sharing as human rights violations. - Highlights psychological, social, and economic consequences of violence in digital contexts. - Calls for states to act urgently to prevent and respond to VAWG in digital contexts.

2023	Commission on the Status of Women (CSW67) Agreed Conclusions	• Focuses on the priority theme: Innovation, technological change, and digital education for gender equality. • Expresses deep concern at the scale and impact of violence against women and girls that occurs or is amplified by the use of technology. • Calls for comprehensive preventive and eliminatory measures targeting gender-based violence in technology-mediated environments.
	UN General Assembly Resolution A/78/213: Human Rights in the Context of Digital Technologies	• Recognises sexual exploitation, harassment, stalking, bullying, non-consensual image sharing as forms of gender-based violence. • Urges states, platforms, and stakeholders to uphold due diligence obligations for preventing harm, especially in artificial intelligence (AI) contexts.
2024	UN General Assembly Resolution A/78/L.49: Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development	• Endorses development of safe and inclusive AI systems. • Identifies malicious use of AI as a risk factor for reinforcing discrimination and structural inequalities, including in relation to gender
	Global Digital Compact (Annex to Pact for the Future)	• Articulates shared principles for inclusive, fair, and safe global digital governance. • Explicitly includes the elimination of sexual and gender-based violence that occurs or is amplified by the use of technology as a core principle. • Emphasises the need for gender mainstreaming across digital policy.
	UN General Assembly Resolution A/RES/79/152: Intensification of Efforts to Eliminate VAWG in Digital Environments	• Recognises the continued prevalence of VAWG across offline and online settings, as well as the interrelation of these settings. • Urges States to take immediate, effective action to prevent and eliminate VAWG that occurs or is amplified by the use of digital technologies, through strengthened legislation, investigation, prosecution and enhanced protection and support for all victims. • Calls for strengthened prevention, regulation of platforms, safety by design and accountability.

	Human Rights Council Resolution A/HRC/RES/56/19 on TF GBV	• Requests a Human Rights Council Advisory Committee study on the impacts of technology-facilitated gender-based violence and global good practices. • Calls for comprehensive legal responses and cross-sector collaboration. • Emphasises coordinated global action involving States, UN entities, civil society, victims, and private sector.
	UN Convention against Cybercrime	• Establishes an international legal framework to combat cybercrime. • Addresses crimes including unauthorised access, fraud, malware, as well as gender-based violence that occurs or is amplified through the use. • of an information and communications technology system. • Calls for the criminalization of the non-consensual dissemination of intimate images. • Supports international cooperation, cross-border evidence sharing, and digital law enforcement coordination.
2025	Human Rights Council, Report of the Special Rapporteur on Violence against Women, Its Causes and Consequences, Sex based violence against women and girls: new frontiers and emerging issues, A/HRC/59/47	• Highlights those emerging technologies, particularly AI, are creating new and intensified forms of online violence against women (TFVAWG), which often remain underreported. • Identifies AI generated deepfakes as an emerging form of sexual exploitation. • Emphasises how digital technologies (e.g. Apps, smart devices) enable increased surveillance and tracking of women. • Notes significant challenges for justice systems, including cross border perpetrators and difficulties in ident
2026	Committee on the Elimination of Discrimination against Women Addendum to General Recommendation No. 30 on women in conflict prevention, conflict and post-conflict situations in relation to the Women Peace and Security agenda	• Recognises emerging technologies (AI, cyberwarfare) as reshaping conflict and introducing cyberspace as a new site of gender-based violence. • Frames technology facilitated violence (TFVAWG) as part of the continuum of GBV, including forms such as deepfakes, sextortion and cyber trafficking. • Highlights the gendered impacts of digital harms, including exclusion from decision making and the chilling effect on women's participation in peacebuilding. • Calls for stronger regulation, private sector accountability and coordinated multi stakeholder responses to address digital violence in conflict setting

Annex Table 2. Regional normative development of TFVAWG

Year	Normative instruments	Key elements related to TF VAWG
1994	Inter-American Convention on the Prevention, Punishment, and Eradication of Violence Against Women (Belém do Pará Convention)	- In 2022, MESECVI issued a report clarifying the original Convention's application to online gender-based violence against women and girls. - MESECVI is developing a Model Law to address online gender-based violence against women and girls through legislative tools.
2003	Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa (Maputo Protocol)	- Adopted in 2003, the Maputo Protocol provides a comprehensive legal framework for setting out African states' obligations to respect, protect and fulfil women's rights, and to hold states accountable for their violation of those rights. - The ACHPR, as the continent's standard setting and monitoring human rights mechanism, has made clear that the Maputo Protocol's provisions also apply to TFVAWG (see below).
2011	Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence (Istanbul Convention) – GREVIO General Recommendation 1 (2021)	- First binding European instrument focused on four pillars: prevention, protection, prosecution and coordinated policies. - GREVIO General Recommendation No. 1 (2021) on the digital dimension of violence against women defines online and technology-facilitated violence against women and girls, including non-consensual image sharing or taking/producing, exploitation, coercion and threats, sexualized bullying, online harassment, stalking, and cyberflashing.
2022	European Union (EU) Digital Services Act	- Sets out new rules for online platforms and digital services operating in the EU. - Requires platforms, small and large, to prevent and address illegal and harmful content, remove non-consensual images that are disseminated online, the spread of disinformation improve transparency around content moderation and algorithmic processes.

2022	African Commission on Human and Peoples' Rights Resolution ACHPR/Res. 522 (LXXII) on the Protection of Women Against Digital Violence in Africa	• Calls on States to expand in their legislation the definition of gender-based violence to include digital violence against women including cyber-harassment, cyberstalking, sexist hate speech amongst other ICT-related violations. • Covers needs for research, awareness-raising programmes, women's and girls' access to digital education, service providers' training, law enforcement and service providers cooperation. • Calls for special measures to protect women journalists from digital violence.
2024	European Union (EU) AI Act	• Requires creators of deepfakes to inform the public about the artificial nature of their work. • Requires providers of general-purpose AI tools to tag AI-generated content and identify manipulations, aiding transparency.
	African Union Convention on Ending Violence Against Women and Girls (AU CEVAWG)	• Recognises violence against women and girls and requires states to adopt legislative, institutional and policy measures; however, it does not expressly define TFVAWG and provides limited detail on platform accountability, algorithmic transparency, content moderation, AI enabled abuse and cross border enforcement.
2025	Resolution on developing Guidelines to assist States to monitor technology companies in respect of their duty to maintain information integrity through independent fact checking - ACHPR/Res.630 (LXXXII)	• Reaffirms that human rights offline must be protected online, including freedom of expression and access to information. • Raises concerns about technology companies' failures in content moderation, particularly regarding African languages, human oversight and AI systems. • Warns against reliance on "community notes" as a substitute for corporate responsibility and independent fact checking, highlighting risks to information integrity and political manipulation. • Calls for stronger corporate accountability, including human rights due diligence, transparency, and the development of guidelines to monitor platform performance, especially in high-risk contexts such as elections and conflict.
	ACHPR Special Rapporteur on the Rights of Women in Africa (SRRWA)- Report presented at the 83rd Ordinary Session of the African Commission on Human and Peoples' Rights	• Emphasises protection and monitoring functions, including reporting on violations, issuing statements and engaging with governments and stakeholders to address women's rights concerns. • Reinforces the need for stronger regional cooperation and accountability mechanisms to advance women's rights, including in emerging areas such as digital harms and conflict related violence.

2026	CoE Recommendation CM/Rec(2026)1 of the Committee of Ministers to member States on equality and artificial intelligence	• Promotes equality, including gender equality and prevents discrimination across the full AI lifecycle: design, deployment, use and retirement. • Focuses on transparency, explainability, procedural safeguards and remedies so people can identify AI related discrimination and access redress.
	Recommendation CM/Rec(2026)2 of the Committee of Ministers to member States on accountability for technology-facilitated violence against women and girls	• Provides guidance for member States on enhancing their legal, institutional and regulatory responses to technology-facilitated violence against women and girls. • Proposes a comprehensive notion of accountability, extending beyond criminal law to civil and administrative fields. • Promotes a victim centred, trauma informed and multi stakeholder approach.



Lawyers
for Justice
in Libya



Centre for
Protecting
Women Online



The Open
University