

*Position paper*

# Digital gender-based violence: strengthening the law, protection and support

## Morocco - Tunisia - Egypt

**Digital technology has become a space where gender-based violence is expressed and amplified.** Far from being separate from offline violence, online violence forms part of the same continuum: it often extends existing violence, but it can also originate online before continuing offline.

In 2022, a group of experts convened by UN Women and the WHO defined **technology-facilitated violence (TFV) as any act "committed, assisted, aggravated or amplified" by digital technologies, causing physical, sexual, psychological, social, political or economic harm.**

This violence thrives in online environments where misogynistic and anti-rights discourse can spread and become normalised. In a context of backlash against gender-related rights, the manosphere and other masculinist communities contribute to structuring, amplifying and normalising anti-feminist discourse, and violence targeting those who stand up for equality. This climate of insecurity can deter those affected from reporting violence or from turning to existing protection mechanisms, widening the gap between the scale of the phenomenon and the responses to it.

**The scale is considerable**: between 16% and 58% of women, depending on the study, have experienced technology-facilitated violence. The law has not kept pace. Fewer than 40% of countries protect women against cyber-harassment and online stalking, leaving 1.8 billion women and girls, or 44% of them worldwide, without access to legal protection.

**Risks are also unevenly distributed**: women activists and LGBTQIA+ persons are among the most exposed, and the rise of generative artificial intelligence is making the threat worse. Yet legislating is not enough, because a poorly designed law can be turned against those it was meant to protect, and a law that is not enforced remains ineffective.

In the SWANA region, the UN Women survey conducted in 2021 among 11,500 internet users in eight countries, including Morocco and Tunisia, reveals both the scale of the phenomenon and the silence that surrounds it. Nearly one in two women internet users (49%) say they do not feel safe from online harassment. Among women who have experienced it, only 31% reported it, and 41% of those who did not report it said they did not think it would make any difference. When they do report, it is first to the platform (55%), well ahead of the police (23%).

In Morocco, Tunisia and Egypt, these dynamics take specific forms but reveal **persistent difficulties in guaranteeing effective protection**. In Morocco, Law 103-13, adopted in 2018, is the main legal framework for combating violence against women, defining and punishing in particular physical, sexual, psychological and economic violence.

In Tunisia, Organic Law 58-2017 establishes a comprehensive framework for the prevention, protection and prosecution of violence against women, but does not explicitly mention digital violence. In Egypt, despite criminal provisions covering several forms of violence and a dedicated national strategy, there is still no unified legislative framework covering all forms of violence against women.

**The law can only address this violence if it recognises it in all its diversity, provides real access to justice, and is backed by services able to inform, protect and support those affected.**

Where these conditions are lacking, feminist organisations and grassroots actors often step in: they document the violence, support victims and build responses grounded in the realities and needs of those affected. Yet, just as needs are growing, their capacity to act is weakened by shrinking funding.

This violence is not inevitable, and States have the means to address it, provided they **strengthen legal frameworks, ensure their effective enforcement and consolidate the organisations that support affected people on a daily basis.**

# Our recommendations

### 1. Close the legal gap on the definition of digital violence

Existing legal frameworks remain insufficiently adapted to contemporary forms of technology-facilitated violence. Legislation must therefore evolve to explicitly define and classify gender-based digital violence and its various manifestations (harassment, threats, non-consensual sharing of intimate content, identity theft, digital tracking or surveillance, among others).

Draw on UN Women's Model Framework for Legislation on Technology-Facilitated Violence against Women and Girls (2025) in all three countries. It sets out principles and standards for adapting national legislation to the different forms of technology-facilitated violence.

### 2. Ensure that legal frameworks cannot be turned against victims

Beyond the absence or inadequacy of specific provisions, existing legal frameworks can themselves create new vulnerabilities when applied extensively or diverted from their protective purpose. In Egypt, Article 25 of Law 175/2018 on cybercrime, which penalises in particular violations of "family values", has thus been used in several prosecutions of women for their online activities or content. In Tunisia, Decree-Law No. 54 has been used in prosecutions targeting, among others, journalists and people who expressed criticism online. In Morocco, the extension of criminal conciliation raises the question of its application to situations of gender-based violence.

Introduce procedural safeguards and protection mechanisms so that recourse to the law cannot expose victims, witnesses or those reporting violence to prosecution, reprisals or further danger.

### 3. Hold digital platforms accountable, in particular for moderation in local languages

UNESCO's Guidelines (2023) recommend content moderation in local languages. Yet, according to X's report under the EU Digital Services Act (November 2023), the platform had 12 Arabic-speaking moderators compared with 2,294 English-speaking ones. Maghrebi Arabic dialects also suffer from insufficient and unrepresentative training data for automated moderation tools (Center for Democracy and Technology, 2024).

Require platforms to publish transparent data, disaggregated by language and dialect, on their moderation capacity.

The removal of non-consensual intimate content should not depend on the victim's ability to identify the perpetrator.

Require a rapid takedown mechanism for non-consensual intimate content, independent of such identification, and accountability for anyone who redistributes it.

### 4. Guarantee comprehensive, coordinated and sustainably funded support for victims

Support for victims remains fragmented and largely dependent on civil society. According to a global UN Women survey (2025) of 428 women's rights and civil society organisations, 34% have suspended or discontinued programmes to end violence against women following funding cuts, and 78% report reduced access to essential services for survivors.

Strengthen and sustain, in all three countries, comprehensive support systems, by improving coordination between public institutions and civil society and ensuring sustainable funding.

### 5. Prevent upstream: make digital education and the engagement of men and boys levers of prevention

27% of the men surveyed in UN Women's regional survey (2021) admit to having themselves committed a form of digital violence.

Make the prevention of digital violence a priority of education and youth policies, involving men and boys as actors in prevention.

### 6. Document and protect LGBTQIA+ persons against targeted digital violence

This violence takes the form of denunciation campaigns, surveillance and digital entrapment, at times involving State actors themselves. Human Rights Watch (2023) documented 45 cases of arrest of LGBT persons in four countries of the region (Egypt, Jordan, Lebanon and Tunisia), where security forces sought to collect, or even create, digital evidence.

Continue, in all three countries, to document the different mechanisms of digital targeting and persecution, in particular online denunciation campaigns, targeting by security forces themselves and entrapment through dating apps, while guaranteeing the safety, confidentiality and anonymity of those concerned.

Any action in this field must be developed with local LGBTQIA+ organisations, without ever creating new risks for the people it seeks to protect.

### 7. Anticipate and document violence linked to generative artificial intelligence

The rise of generative AI tools facilitates new forms of digital violence, including the creation and dissemination of non-consensual intimate images, deepfakes, identity theft and the automation of harassment. These practices can cause serious sexual, psychological, social and professional harm, while the speed at which they are produced and spread makes them harder to prevent and to respond to.

Integrate these forms of violence now into prevention, documentation, protection and redress systems, by developing data on their scale and manifestations and adapting legal frameworks and reporting mechanisms to the specific features of AI-generated or manipulated content.

### 8. Build on international commitments already ratified

Among the three countries, only Morocco and Tunisia have ratified the Optional Protocol to CEDAW. Tunisia ratified the Maputo Protocol in 2018, while Morocco and Egypt have not ratified it. Morocco and Tunisia are parties to the Budapest Convention on Cybercrime, unlike Egypt, which is instead a party to the Arab Convention on Combating Information Technology Offences.

Mobilise existing international commitments as levers for reform and accountability, beyond calling for new legislation. Draw on CEDAW monitoring mechanisms, individual communications where admissibility conditions are met, and the Universal Periodic Review (UPR), to document gaps between States' commitments and their implementation, raise the visibility of gender-based digital violence and put forward concrete reform recommendations. In Morocco and Tunisia, also use the Budapest Convention on Cybercrime, to which both countries are parties, as a lever to promote the adaptation of national legislation and strengthen cross-border cooperation on investigations and electronic evidence.