

Note de positionnement

Violences numérique de genre : Renforcer le droit, la protection et l'accompagnement

Maroc - Tunisie - Égypte

Le numérique est devenu un espace où les violences fondées sur le genre s'expriment et s'amplifient. Loin d'être séparées des violences hors ligne, les violences en ligne s'inscrivent dans un même continuum : elles prolongent souvent des violences existantes, mais peuvent aussi naître en ligne avant de se poursuivre hors ligne.

En 2022, un groupe d'experts réuni par ONU Femmes et l'OMS a défini les **violences facilitées par la technologie (VFFT) comme tout acte « commis, facilité, aggravé ou amplifié » par les technologies numériques, causant un préjudice physique, sexuel, psychologique, social, politique ou économique.**

Ces violences prospèrent dans des environnements en ligne où les discours misogynes et anti-droits peuvent se diffuser et se banaliser. Dans un contexte de recul des droits liés au genre, la manosphère et d'autres communautés masculinistes participent à structurer, amplifier et normaliser des discours antiféministes, et des violences visant celles et ceux qui revendiquent l'égalité. Ce climat d'insécurité peut dissuader les personnes concernées de signaler les violences ou de recourir aux mécanismes de protection existants, et creuse l'écart entre l'ampleur du phénomène et les réponses qui lui sont apportées.

L'ampleur est considérable : entre 16 % et 58 % des femmes, selon les études, ont déjà subi des violences facilitées par la technologie. Le droit n'a pas suivi. Moins de 40 % des pays protègent les femmes contre le cyberharcèlement et la traque en ligne, ce qui laisse 1,8 milliard de femmes et de filles, soit 44 % d'entre elles dans le monde, sans accès à une protection juridique.

Les risques ne sont d'ailleurs pas répartis également : les militantes et les personnes LGBTQIA+ sont parmi les plus exposées, et l'essor de l'intelligence artificielle générative aggrave encore la menace. Or légiférer ne suffit pas, car une loi mal conçue peut se retourner contre celles qu'elle devait protéger, et une loi qui n'est pas appliquée reste sans effet.

Dans la région SWANA, l'enquête d'ONU Femmes menée en 2021 auprès de 11 500 internautes dans huit pays, dont le Maroc et la Tunisie, révèle à la fois l'ampleur du phénomène et le silence qui l'entoure. Près d'une internaute sur deux (49 %) dit ne pas se sentir en sécurité face au harcèlement en ligne. Parmi les femmes qui en ont été victimes, seules 31 % ont signalé les faits, et celles qui ne l'ont pas fait expliquent à 41 % qu'elles ne pensaient pas que cela changerait quoi que ce soit. Quand elles signalent, c'est d'abord à la plateforme (55 %), bien avant la police (23 %).

Au Maroc, en Tunisie et en Égypte, ces dynamiques prennent des formes spécifiques, mais révèlent des **difficultés persistantes à garantir une protection effective**. Au Maroc, la loi 103-13, adoptée en 2018, constitue le principal cadre légal de lutte contre les violences faites aux femmes, en définissant et en réprimant notamment les violences physiques, sexuelles, psychologiques et économiques.

En Tunisie, la loi organique 58-2017 établit un cadre global de prévention, de protection et de poursuite des violences faites aux femmes, mais ne mentionne pas explicitement les violences numériques. En Égypte, malgré des dispositions pénales couvrant plusieurs formes de violences et une stratégie nationale dédiée, il n'existe toujours pas de cadre législatif unifié couvrant l'ensemble des violences faites aux femmes.

Le droit ne peut répondre à ces violences que s'il les reconnaît dans leur diversité, ouvre un accès réel à la justice et s'accompagne de dispositifs capables d'informer, de protéger et d'accompagner.

Lorsque ces conditions font défaut, les organisations féministes et les actrices de terrain prennent le relais : elles documentent les violences, accompagnent les victimes et construisent des réponses ancrées dans les besoins des personnes concernées. Pourtant, alors que les besoins augmentent, la contraction des financements fragilise leur capacité d'action.

Ces violences ne sont pas une fatalité, et les États ont les moyens d'y répondre, à condition de **renforcer les cadres juridiques, d'en garantir l'application concrète et de consolider les organisations qui accompagnent les personnes au quotidien.**

Nos recommandations

1. Combler le vide juridique sur la définition des violences numériques

Les cadres juridiques existants restent insuffisamment adaptés aux formes contemporaines de violences facilitées par les technologies. Il s'agit donc de faire évoluer les législations afin de définir et qualifier explicitement les violences numériques fondées sur le genre, ainsi que leurs différentes manifestations (harcèlement, menaces, diffusion non consentie de contenus intimes, usurpation d'identité, traçage ou surveillance numérique, entre autres).

S'appuyer, dans les trois pays, sur le Model Framework for Legislation on Technology-Facilitated Violence against Women and Girls d'ONU Femmes (2025), qui propose des principes et standards pour adapter les législations nationales aux différentes formes de violences facilitées par les technologies.

2. Garantir que les cadres juridiques ne puissent être détournés contre les victimes

Au-delà de l'absence ou de l'insuffisance de dispositions spécifiques, les cadres juridiques existants peuvent eux-mêmes produire de nouvelles vulnérabilités lorsqu'ils sont appliqués de manière extensive ou détournés de leur finalité protectrice. En Égypte, l'article 25 de la loi 175/2018 sur la cybercriminalité, qui sanctionne notamment les atteintes aux « valeurs familiales », a ainsi été utilisé dans plusieurs poursuites visant des femmes pour leurs activités ou contenus en ligne. En Tunisie, le décret-loi n°54 a été utilisé dans des poursuites visant notamment des journalistes et des personnes ayant exprimé des critiques en ligne. Au Maroc, l'extension de la conciliation pénale soulève la question de son application aux situations de violences fondées sur le genre.

Introduire des garanties procédurales et des mécanismes de protection afin que le recours au droit ne puisse exposer les victimes, témoins ou personnes dénonçant des violences à des poursuites, à des représailles ou à une mise en danger supplémentaire.

3. Responsabiliser les plateformes numériques, notamment en matière de modération dans les langues locales

Les lignes directrices de l'UNESCO (2023) recommandent une modération des contenus dans les langues locales. Or, selon le rapport de X au titre du règlement européen sur les services numériques (novembre 2023), la plateforme comptait 12 modérateurs arabophones contre 2 294 anglophones. Les dialectes arabes maghrébins souffrent en outre de données d'entraînement insuffisantes et peu représentatives pour les outils automatisés de modération (Center for Democracy and Technology, 2024).

Exiger des plateformes la publication de données transparentes et désagrégées par langue et par dialecte sur leurs capacités de modération. Le retrait d'un contenu intime non consenti ne devrait pas dépendre de la capacité de la victime à identifier son agresseur.

Exiger un mécanisme de retrait rapide des contenus intimes non consentis, indépendant de cette identification, et une responsabilité engagée pour toute personne qui les rediffuse.

4. Garantir une prise en charge globale, coordonnée et durablement financée des victimes

La prise en charge des victimes reste fragmentée et largement dépendante de la société civile. Selon une enquête mondiale d'ONU Femmes (2025) auprès de 428 organisations de défense des droits des femmes et de la société civile, 34 % ont suspendu ou arrêté des programmes de lutte contre les violences faites aux femmes à la suite de coupes de financement, et 78 % rapportent une réduction de l'accès des survivantes aux services essentiels.

Renforcer et pérenniser, dans les trois pays, des dispositifs de prise en charge globale, en améliorant la coordination entre institutions publiques et société civile, et en garantissant un financement durable.

5. Prévenir en amont : faire de l'éducation numérique et de l'engagement des hommes et des garçons des leviers de prévention

27 % des hommes interrogés dans l'enquête régionale d'ONU Femmes (2021) reconnaissent avoir eux-mêmes commis une forme de violence numérique.

Faire de la prévention des violences numériques un axe prioritaire des politiques éducatives et de jeunesse, en associant les hommes et les garçons comme acteurs de la prévention.

6. Documenter et protéger les personnes LGBTQIA+ face aux violences numériques ciblées

Ces violences prennent la forme de campagnes de dénonciation, de surveillance et de piégeage numérique, parfois avec l'implication d'acteurs étatiques eux-mêmes. Human Rights Watch (2023) a documenté 45 cas d'arrestation de personnes LGBT dans quatre pays de la région (Égypte, Jordanie, Liban et Tunisie), où les forces de sécurité ont cherché à collecter, voire à créer, des preuves numériques.

Poursuivre, dans les trois pays, la documentation des différents mécanismes de ciblage et de persécution numérique, notamment les campagnes de délation numérique, le ciblage mené par les forces de sécurité elles-mêmes et le piégeage via les applications de rencontre, en garantissant la sécurité, la confidentialité et l'anonymat des personnes concernées.

Toute action dans ce domaine doit être construite avec les organisations LGBTQIA+ locales, sans jamais créer de nouveaux risques pour les personnes que l'on cherche à protéger.

7. Anticiper et documenter les violences liées à l'intelligence artificielle générative

L'essor des outils d'intelligence artificielle générative facilite de nouvelles formes de violences numériques, notamment la création et la diffusion d'images intimes non consenties, de deepfakes, l'usurpation d'identité ou encore l'automatisation du harcèlement. Ces pratiques peuvent produire des préjudices sexuels, psychologiques, sociaux et professionnels importants, tandis que leur rapidité de production et de diffusion complique leur prévention et leur prise en charge.

Intégrer dès à présent ces formes de violences dans les dispositifs de prévention, de documentation, de protection et de recours, en développant des données sur leur ampleur et leurs manifestations et en adaptant les cadres juridiques et les mécanismes de signalement aux spécificités des contenus générés ou manipulés par IA.

8. S'appuyer sur les engagements internationaux déjà ratifiés

Parmi les trois pays, seuls le Maroc et la Tunisie ont ratifié le Protocole facultatif à la CEDEF. La Tunisie a ratifié le Protocole de Maputo en 2018, tandis que le Maroc et l'Égypte ne l'ont pas ratifié. Le Maroc et la Tunisie sont parties à la Convention de Budapest sur la cybercriminalité, contrairement à l'Égypte, qui est en revanche partie à la Convention arabe relative à la lutte contre les délits informatiques.

Mobiliser les engagements internationaux existants comme leviers de réforme et de redevabilité, au-delà de la demande d'adoption de nouveaux textes. S'appuyer sur les mécanismes de suivi de la CEDEF/CEDAW, les communications individuelles lorsque les conditions de recevabilité sont réunies, ainsi que sur l'Examen périodique universel (EPU), pour documenter les écarts entre les engagements des États et leur mise en œuvre, renforcer la visibilité des violences numériques fondées sur le genre et porter des recommandations concrètes de réforme. Au Maroc et en Tunisie, mobiliser également la Convention de Budapest sur la cybercriminalité, à laquelle les deux pays sont parties, comme levier pour promouvoir l'adaptation des législations nationales et renforcer la coopération transfrontalière en matière d'enquête et de preuves électroniques.



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.