Funded by
the European Union

EU4GenderEquality
Reform Helpdesk
PHASE II

Technology-Facilitated Gender-Based Violence (TFGBV)

Good Practices from Eastern Partnership Countries in Light of EU Directive 2024/1385

Prepared for the Eastern Partnership Working Group on Gender Equality

EXECUTIVE SUMMARY

Technology-facilitated gender-based violence (TFGBV) has emerged as a critical challenge affecting women and girls across the Eastern Partnership region. As digitalisation reshapes political, economic, and social life, women are increasingly exposed to online harassment, cyberstalking, non-consensual dissemination of intimate images (including deepfakes), digital surveillance, and coordinated disinformation campaigns. Research across the region confirms the severity of this phenomenon: a UN Women study surveying over 12,000 women across Eastern Europe and Central Asia found that more than half (53.2%) of women present online have experienced some form of technology-facilitated violence in their lifetime, with prevalence reaching as high as 76.8% in Ukraine and 72.4% in Türkiye.[1] TFGBV undermines gender equality, restricts women's participation in public and political life, and poses a direct challenge to fundamental rights, democratic governance, and the rule of law.

The adoption of EU Directive 2024/1385 on combating violence against women and domestic violence marks a significant milestone, establishing for the first time EU-wide criminal offences for specific forms of cyber violence. This development is reinforced by a strengthening global normative framework, including UN General Assembly Resolution A/RES/79/152 (2024) on eliminating violence against women in the digital environment, the Global Digital Compact (2024) naming gender equality and countering technology-facilitated violence as core principles of digital governance, and Human Rights Council Resolution A/HRC/56/L.15 (2024) on technology-facilitated gender-based violence.[2] For Eastern Partnership countries, particularly EU candidate countries, these developments present a timely opportunity to align national legislation and institutional practice with European and international standards, complementing obligations under the Council of Europe Istanbul Convention and GREVIO General Recommendation No. 1 on the digital dimension of violence against women.

This background paper situates TFGBV within the broader framework of the EU Gender Action Plan III (2021–2025), demonstrating its relevance across all three thematic priorities: ending gender-based violence; promoting women's participation and leadership; and advancing women's economic and social rights in the digital age. It further

[1] UN Women Europe and Central Asia Regional Office, *The Dark Side of Digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia* (2023), Executive Summary, p. 4.
[2] UN Women, *Repository of UN Women's Work on Technology-Facilitated Violence Against Women and Girls* (March 2025), p. 2.

highlights the importance of TFGBV as an EU Enlargement and fundamental rights issue, linked to access to justice, institutional accountability, and protection of democratic participation.

Drawing on examples from Armenia, Azerbaijan, Belarus, Georgia, Moldova, and Ukraine, the paper highlights emerging good practices, including Moldova's comprehensive legislative reforms criminalising digital violence and its pioneering multi-stakeholder Technical Group of Experts on TFGBV, Ukraine's capacity-building efforts despite the ongoing war, and Georgia's institutional measures following GREVIO recommendations. At the same time, it identifies persistent challenges across the region, including fragmented legal frameworks, limited institutional coordination, insufficient survivor-centred digital services, and a lack of disaggregated and comparable data on TFGBV.

Critically, the paper addresses all dimensions requiring strengthened attention. The effective prevention requires a whole-of-society approach engaging governments, civil society, the education sector, media, and communities in addressing the root causes of digital violence against women.[3] This includes integrating digital literacy and gender perspectives into education curricula, engaging men and boys in understanding the consequences of TFGBV, promoting media responsibility in reporting on digital violence, and strengthening multistakeholder coordination at national and international levels through mechanisms such as the Generation Equality Action Coalitions and the Global Partnership for Action on Gender-Based Online Harassment and Abuse.[4]

Digital platform accountability is central to any comprehensive strategy. Research confirms that Facebook and Instagram are the platforms where women most frequently experience TFGBV, yet platforms' standards and trust and safety policies provide limited provision for gender-sensitive responses, make little reference to relevant human rights frameworks, and lack sex-disaggregated data on cyber violence incidents.[5] The EU Digital Services Act provides a regulatory model, which recommends to advocate for platforms to incorporate gender-sensitive approaches, implement harmonised definitions of TFGBV, design reporting systems that collect sex-disaggregated data, and enhance cooperation with law enforcement.[6]

The paper also highlights significant barriers to reporting: only 7.1% of women who experience TFGBV report to police, primarily due to beliefs that nothing will be done, lack of trust in institutions, and fear of being blamed. At the same time, 70.4% of women want stronger accountability from platform companies, 66.5% want more effective institutional protection, and 69.7% want awareness-raising to empower women to prevent and counter TFGBV.[7] These findings should guide policy priorities.

The paper identifies specific actions that could be taken to address the problem with targeted suggestions for EaP governments and EU partners across six areas: (1) legislative alignment with EU Directive 2024/1385; (2) strengthened institutional capacity including specialised training and online reporting mechanisms; (3) survivor-centred digital response mechanisms; (4) prevention and awareness measures including digital citizenship education; (5) whole-of-society prevention strategies engaging all stakeholders; and (6) digital platform accountability through advocacy, regulation, and multistakeholder engagement. It underscores that addressing technology-facilitated

[3] UN Women ECA, *The Dark Side of Digitalization* (2023), p. 7.
[4] UN Women, *Repository of UN Women's Work on Technology-Facilitated Violence Against Women and Girls* (March 2025), p. 1; UN Women ECA, *The Dark Side of Digitalization* (2023), p. 7.
[5] European Institute for Gender Equality (EIGE), *Tackling cyber violence against women and girls: The role of digital platforms* (Luxembourg: Publications Office of the European Union, 2024), pp. 5, 10.
[6] Ibid., pp. 16-17.
[7] UN Women ECA, *The Dark Side of Digitalization* (2023), Executive Summary, p. 5.

gender-based violence is no longer a peripheral digital safety concern but a core gender equality, rule of law, and democratic governance priority for the Eastern Partnership, requiring coordinated and sustained EU engagement grounded in GAP III, aligned with EU legal standards, and embedded in Enlargement and Association processes.

1. Understanding Technology-Facilitated Gender-Based Violence

Technology-facilitated gender-based violence (TFGBV) has emerged as a critical barrier to gender equality, democratic participation, and fundamental rights across the Eastern Partnership region. As digitalisation accelerates in public, political, and economic life, women and girls are increasingly exposed to online harassment, surveillance, non-consensual dissemination of intimate images, deepfake abuse, and coordinated disinformation campaigns. Addressing TFGBV is therefore integral to the implementation of the EU Gender Action Plan III (2021–2025), the EU's external action priorities on human rights and democracy, and the Enlargement fundamentals related to rule of law, fundamental rights, and inclusive governance.

1.1 Definition and Scope

TFGBV, also referred to as digital violence or cyber violence against women, encompasses any act of violence committed, assisted, aggravated, or amplified by the use of information and communication technologies (ICT) or digital tools against a person on the basis of their gender. According to GREVIO General Recommendation No. 1 (2021) on the digital dimension of violence against women, this term is comprehensive enough to comprise both online acts of violence and those perpetrated through technology, including technology yet to be developed.

TFGBV exists on a continuum with offline gender-based violence and often facilitates, extends, or exacerbates physical violence.

Comprehensive research across the Eastern Europe and Central Asia region confirms the significant prevalence of TFGBV. A UN Women study surveying over 12,000 women across 13 countries found that more than half (53.2%) of women present online have experienced some form of technology-facilitated violence in their lifetime, with prevalence reaching as high as 76.8% in Ukraine and 72.4% in Türkiye.[8] The most common forms include receiving unwanted or offensive content or messages (39.7%), inappropriate sexual advances on social media (30%), and account hacking (25.4%).[9]

Certain groups face heightened risks: younger women aged 18-24 are four times more likely to experience TFGBV than women over 65; LGBTQI+ women, women from urban areas, and divorced women also face elevated risk.[10] Significantly, while the majority of TFGBV is perpetrated by unknown persons (50.3%), nearly one-third (32.1%) is perpetrated by persons in women's social proximity—partners, family members, friends, or colleagues—demonstrating the continuum between online and offline violence.[11]

[8] UN Women Europe and Central Asia Regional Office, *The Dark Side of Digitalization: Technology-facilitated violence against women in Eastern Europe and Central Asia* (2023), Executive Summary, p. 4.
[9] Ibid., p. 4.
[10] Ibid., p. 5.
[11] Ibid., p. 4-5.

1.2 Common Forms of TFGBV

TFGBV manifests in multiple forms, including:

Form of TFGBV	Description
Non-consensual intimate image sharing	Sharing intimate or sexually explicit images/videos without consent, including deepfakes
Cyberstalking	Persistent monitoring, surveillance, or following through digital means, including use of tracking apps and spyware
Online harassment	Threatening, insulting, or intimidating communications targeting an individual or group
Doxxing	Publishing private personal information (address, phone, workplace) to enable harassment or violence
Sextortion	Blackmail using threats to publish sexual information, images or videos
Cyber incitement to hatred	Online content promoting hatred or violence based on sex or gender

The forms of TFGBV listed align with those identified in global research, including UN Women's Joint Programme on Violence against Women Data with the World Health Organization, which has developed a common definition characterising technology-facilitated violence against women as "any act that is committed, assisted, aggravated or amplified by the use of ICTs or other digital tools, that results in or is likely to result in physical, sexual, psychological, social, political or economic harm, or other infringements of rights and freedoms."[12]

The prevention of and response to TFGBV contributes to several key thematic areas of engagement under the EU GAP III. In particular, TFGBV directly undermines the objective of ensuring freedom from all forms of gender-based violence and access to justice, especially where legal frameworks and institutional responses lag behind technological developments. It also constrains women's equal participation and leadership in public and political life, including in electoral processes, media, and civic activism. Moreover, TFGBV negatively affects the realisation of women's economic and social rights by limiting access to digital skills, economic opportunities, and safe participation in the digital economy. Addressing TFGBV therefore constitutes a cross-cutting implementation concern across GAP III thematic areas, including in the context of EU engagement in the Eastern Partnership.

2. EU Directive 2024/1385: A New European Framework

On 14 May 2024, the European Union adopted Directive (EU) 2024/1385 on combating violence against women and domestic violence, representing the first EU legislation to specifically address these issues comprehensively. Member States have until 14 June 2027 to transpose the Directive into national law.

[12] UN Women, *Expert Group Meeting report: Technology-facilitated violence against women: Towards a common definition* (2023), as cited in UN Women ECA, *The Dark Side of Digitalization* (2023), p. 2.

2.1 Key Provisions on Cyber Violence

The Directive introduces EU-wide criminal offences for specific forms of cyber violence, filling critical gaps that were not expressly addressed by the Council of Europe Istanbul Convention. The criminalised offences include:

Non-consensual sharing of intimate or manipulated material (including deepfakes and AI-generated content)

Cyberstalking (persistent surveillance, monitoring, or following using digital tools)

Cyber harassment (threatening or intimidating conduct via electronic means)

Cyber incitement to hatred or violence (on the grounds of sex or gender)

The EU Directive builds upon and complements a strengthening global normative framework on TFGBV. The UN General Assembly Resolution A/RES/79/152 (2024) on intensifying efforts to prevent and eliminate all forms of violence against women and girls in the digital environment provides a comprehensive framework calling upon States to strengthen legislation, support victims and survivors, enhance digital literacy, and importantly, to refrain from using artificial intelligence systems that pose undue risks to human rights.[13] The Global Digital Compact (2024), adopted as an annex to the Pact for the Future, names gender equality and countering technology-facilitated sexual and gender-based violence as core principles of global digital governance.[14] Additionally, the Human Rights Council Resolution A/HRC/56/L.15 (2024) specifically requests a study on TF GBV and its impact on women and girls, signalling growing international attention to this issue.[15]

2.2 Additional Requirements

Beyond criminalisation, the Directive requires Member States to ensure survivors can report cybercrimes online through accessible, safe channels, including the ability to submit digital evidence such as screenshots. Law enforcement and judicial authorities must have adequate expertise and effective tools to gather, analyse, and secure electronic evidence. The Directive also mandates training for professionals handling such cases and requires data collection on cyber violence offences.

2.3 Relevance for EaP Countries

For EaP countries, alignment with the Directive represents an opportunity and a necessity for Moldova and Ukraine as EU candidate countries.

The Directive sets a benchmark for comprehensive legislation on TFGBV that complements existing Istanbul Convention obligations. Countries that have ratified the Istanbul Convention already have a foundation for addressing the digital dimension of violence through GREVIO General Recommendation No. 1 (2021), which provides detailed guidance on applying Convention provisions to online and technology-facilitated violence.

For EU candidate and associated countries, effective action against technology-facilitated violence against women constitutes an increasingly important component of rule of law and fundamental rights commitments. Gaps in criminalisation, investigation, prosecution, and survivor protection in cases of TFGBV reflect broader challenges related to institutional accountability, access to justice, and protection of fundamental freedoms. Aligning national legislation and practice with the Istanbul Convention, GREVIO General Recommendation No. 1, and Directive (EU) 2024/1385 provides a concrete pathway for Eastern Partnership

[13] UN Women, *Repository of UN Women's Work on Technology-Facilitated Violence Against Women and Girls* (March 2025), p. 2.
[14] Ibid., p. 2.
[15] Ibid., p. 2.

countries that are on the EU accession track - Moldova and Ukraine - to demonstrate progress under the Enlargement fundamentals and EU approximation processes.

3. Good Practices from Eastern Partnership Countries

Across the Eastern Partnership region, TFGBV increasingly targets women in politics, journalism, human rights advocacy, and local governance. Online harassment, coordinated smear campaigns, and AI-enabled manipulation are used to discredit women's leadership, silence dissenting voices, and deter women's participation in public life. In contexts of democratic backsliding and shrinking civic space, TFGBV functions as a gendered form of political intimidation. Addressing TFGBV is therefore essential to safeguarding women's political participation, media freedom, and inclusive democratic processes, in line with EU priorities on democracy support and resilience.

3.1 Republic of Moldova: Landmark Legislative Reforms

> **KEY ACHIEVEMENT:** Moldova has adopted the most comprehensive legal framework on digital violence in the EaP region, with new amendments entering into force on 14 February 2026.

Moldova has taken a pioneering position in the Eastern Partnership region by criminalising digital violence and introducing comprehensive legal protections. In 2025, Moldova revised its Law No. 45/2007 on Preventing and Combating Family Violence to explicitly recognise digital violence as a distinct form of violence against women. The revision introduces definitions for digital violence as any act of harm committed through information technologies or electronic communications.

Key elements of Moldova's approach include:

Criminalisation of stalking: Stalking, including through digital means, is now a criminal offence punishable by up to two years in prison (three years if committed by a family member).

Enhanced penalties for online sexual harassment: Penalties have doubled, with fines up to USD 3,000, community work of 120-240 hours, or up to four years imprisonment (seven years if the victim is a minor).

Comprehensive coverage: The law covers harassment and threats through information technologies, repeated unwanted contact via any means, and online monitoring or surveillance.

Technical Group of Experts: Moldova has established a multi-stakeholder Technical Group of Experts on TFGBV, bringing together government, parliament, tech companies, and civil society. Moldova's Technical Group of Experts on TFGBV reflects emerging best practice in multistakeholder coordination. Research emphasises that at the national level, all stakeholders must strengthen cooperation and coordination to achieve a robust multisectoral approach, and that cybercrime police, where mandated with investigating TFGBV, should be systematically integrated into multisectoral mechanisms.[16]

Capacity building: The National Agency for Prevention and Combating Violence has planned comprehensive training for police, prosecutors, and judges in 2026.

[16] UN Women ECA, *The Dark Side of Digitalization* (2023), p. 8.

Additionally, from 1 January 2026, Moldova's Labour Code includes new provisions on preventing and combating violence and harassment in the workplace, including through electronic communication means, aligning with ILO Convention No. 190.

3.2 Ukraine: Building Capacity Despite the War

Despite the ongoing war, Ukraine has made progress in addressing TFGBV, particularly following its ratification of the Istanbul Convention in 2022. The Council of Europe, through its COVAW (Combating Violence against Women in Ukraine) projects, has supported legislative development and capacity building.

Key developments include:

Legislative amendments: Article 173.7 of the Code of Administrative Offenses now provides for liability for sexual harassment through electronic communications.

Guidance materials: The Council of Europe publication on emerging practices in investigation and prosecution of digital violence against women has been translated into Ukrainian to support law enforcement and judicial professionals.

Research and documentation: Civil society organisations, including Women in Media NGO, have documented patterns of online violence against women journalists, identifying forms such as online defamation, sexism and misogyny, death threats, doxxing, and cyberstalking.

Challenges remain: 81% of women journalists surveyed have experienced digital attacks[17]. However, most forms of TFGBV such as doxxing, deepfakes, or cyberstalking are not yet specifically criminalized in legislation, presenting opportunities for further legislative reform[18].

3.3 Georgia: Legislative Framework and GREVIO Recommendations

Georgia ratified the Istanbul Convention in 2017 and has made amendments to its domestic violence law (renamed the Law on Violence Against Women and/or Elimination of Domestic Violence, Protection and Support of Victims of Violence). The country has criminalised stalking under its Criminal Code.

Developments[19] include:

Prosecution guidelines: The Prosecutor's Office of Georgia has developed guidelines on investigating and supervising cases of gender-based violence against women, including sexual crimes.

Training programmes: By 2024, 35 training activities on sexual harassment prevention have been conducted for prosecutors, investigators, and other staff[20].

Council of Europe support: CoE project supported implementation of GREVIO recommendations, including on the digital dimension of violence[21].

---

[17] Women in Media NGO (Ukraine), "Her Voice, Their Target: Gendered Online Violence Against Ukrainian Women Journalists" (2025), available at: https://wim.org.ua/en/materials/online-gbv/

[18] Marta Pavlyshyn, JurFem: Education Center, as cited in Ukrainian Feminist Network, "Digital attacks against women in the media: a new reality and old inequality" (November 2025), available at: https://www.uafem.net/en/digital-attacks-against-women-in-the-media-a-new-reality-and-old-inequality/

[19] The referenced developments took place before the “Foreign Agents’ law”, Georgian FARA and other legislative changes removing “gender” from Georgian legislation were adopted.

[20] Prosecutor's Office of Georgia, State Report submitted to GREVIO under the First Thematic Evaluation Procedure (2025), GREVIO/INF(2025)12, available at: https://rm.coe.int/grevio-inf-2025-12-state-report-first-thematic-evaluation-georgia/4880289a47

[21] Council of Europe, "Reinforcing gender equality and implementing GREVIO recommendations to combat violence against women and domestic violence in Georgia" (Council of Europe Gender Equality Division, 2023-2026), available at: https://www.coe.int/en/web/genderequality/test-a . See also GREVIO, Baseline Evaluation Report: Georgia (Strasbourg: Council of Europe, November 2022).

However, recent political developments have created significant challenges for continued progress on gender equality and violence against women. The adoption of the Law on Transparency of Foreign Influence in 2024, widely referred to as the “foreign agents’ law,” has placed civil society organisations, including those providing critical services to survivors of gender-based violence and advocating for women’s rights, under restrictive reporting requirements and heightened government scrutiny, threatening their operational capacity and deterring international partnerships. The shrinking civic space, combined with the de facto halt of Georgia’s EU accession process, risks undermining the institutional reforms and capacity-building efforts initiated under GREVIO recommendations and EU-supported programmes, including those addressing the digital dimension of violence against women.

GREVIO's baseline evaluation of Georgia noted the need for stronger measures to address digital violence, and the ongoing Council of Europe project is supporting these efforts through capacity building and awareness-raising activities, including public lectures on combating gender bias in technology.

3.4 Armenia: Emerging Framework on Digital Violence

Armenia has made progress in recognising digital violence as a significant concern. In October 2024, the Council of Europe published a comprehensive study on the Digital Dimension of Violence Against Women in Armenia, identifying gaps and providing recommendations for further reforms.

Key findings and developments:

Criminalisation of cyberstalking: Armenia has criminalised cyberstalking as a specific offence.

Research gaps identified: 78% of legal professionals surveyed acknowledge that current laws do not sufficiently address emerging forms of digital violence[22].

Parliamentary engagement: Members of Armenia's National Assembly have emphasised the need for further legislative improvements specifically targeting digital violence.

Digital platform development: The study findings will help shape Armenia's development of a digital platform for tracking domestic violence cases.

In March 2025, partners convened in Yerevan to discuss the study recommendations and participate in training on digital aspects of violence against women, reviewing best practices and examining case studies[23].

3.5 Azerbaijan: Legislative and Institutional Frameworks

Azerbaijan has established a National Action Plan for Combating Domestic Violence (2020-2023) and maintains legislation promoting gender equality and combating domestic violence. The Council of Europe and EU have been key partners in raising awareness of the Istanbul Convention and supporting legislative alignment with European standards.

Key features:

[22] Council of Europe, "Digital Dimension of Violence Against Women in the Republic of Armenia" (Yerevan: Council of Europe, October 2024), produced under the project "Ending Violence Against Women and Promoting Gender Equality in Armenia," available at: https://rm.coe.int/digital-dimension-of-violence-against-women-in-armenia/1680b1d393

[23] Council of Europe, "Combating digital dimension of violence against women in Armenia: exploring solutions and overcoming challenges" (Council of Europe Gender Equality Division, 11 March 2025), available at: https://www.coe.int/en/web/genderequality/-/combating-digital-dimension-of-violence-against-women-in-armenia-exploring-solutions-and-overcoming-challenges

Legal framework: Laws exist to promote gender equality and combat domestic violence, with equal rights provisions in the Labour Code, Family Code, and Criminal Code.

Gap analysis conducted: The Council of Europe project produced a gap analysis of legislative and policy frameworks on violence against women in line with CoE and international standards[24].

Civil society engagement: Civil society workshops in Baku have engaged representatives on issues related to gender equality and violence against women.

3.6 Belarus: Civil Society Initiatives

Due to the political context, international cooperation with government authorities is limited. However, the EU continues to support civil society organisations working on gender equality.

The systemic repression of independent civil society, media, and human rights defenders since 2020 has severely constrained the space for domestic advocacy on gender equality and violence against women, forcing many organisations and activists into exile. Women human rights defenders and journalists have been disproportionately targeted by state authorities, including through technology-facilitated means such as surveillance, doxxing, and coordinated online harassment campaigns, illustrating how TFGBV can function as a tool of political repression in authoritarian contexts.

Notable initiatives:

Advocacy capacity building: Training programmes in 2025 have strengthened the advocacy capacities of Belarusian feminist, human rights and community-based civil society organisations to advance gender equality.

Digital skills programmes: EU-funded programmes like "Login to Tech" provide educational opportunities for women in IT, contributing to digital empowerment and safety awareness.

4. Ways Forward

While several Eastern Partnership countries have developed specialised mechanisms to address violence against women, responses to TFGBV remain fragmented and insufficiently integrated into national gender-based violence and democratic governance frameworks. TFGBV is frequently treated as an isolated cybercrime or online safety issue, rather than as a form of gender-based violence that also functions as a tool of intimidation, exclusion, and democratic interference. In practice, TFGBV is increasingly deployed through coordinated campaigns by non-state and, in some cases, state-linked actors, including in the context of elections, political participation, and foreign information manipulation and interference (FIMI), as evidenced in recent cases across the region.

Addressing TFGBV therefore requires a comprehensive approach combining resilience (strengthening societal, institutional, and individual capacity to withstand gendered online abuse), resistance (detecting, attributing, and responding to coordinated attacks targeting women in public life), and regulation (ensuring effective legal frameworks, accountability mechanisms, and platform governance). Strengthened coordination between law enforcement, prosecution services, equality bodies, victim support services, electoral

[24] Council of Europe, *"Gap analysis of the legislative and policy framework in the field of violence against women and domestic violence in Azerbaijan in line with the Council of Europe and other international standards"* (Baku: Council of Europe, 2020-2023), produced under the Partnership for Good Governance II (PGG II) Programme project "Raising awareness of the Istanbul Convention and other gender equality standards in Azerbaijan." See also EU4Gender Equality Reform Helpdesk, *Country Gender Profile: Azerbaijan* (December 2023), available at: https://euneighbourseast.eu/wp-content/uploads/2024/11/eu4genderhelpdesk_azerbaijan_countrygenderprofile_2023-cgp_v2.pdf

authorities, media regulators, and digital platforms is essential to deliver coherent prevention, protection, and accountability mechanisms in line with EU standards and democratic values.

Based on the analysis of EU Directive 2024/1385 requirements, GREVIO General Recommendation No. 1, and emerging practices across the EaP region, the following should be considered:

4.1 Adopt further Legislative Measures

1. Adopt comprehensive definitions of digital violence/TFGBV in national legislation, covering all forms identified in EU Directive 2024/1385 and GREVIO General Recommendation No. 1.

2. Specifically criminalise: non-consensual intimate image sharing (including deepfakes), cyberstalking, cyber harassment, doxxing, and cyber incitement to hatred or violence based on sex/gender.

3. Ensure penalties are effective, proportionate, and dissuasive, with enhanced sanctions when victims are minors or the perpetrator is a family member.

4. Extend workplace harassment legislation to explicitly cover digital and electronic communications.

4.2 Enhance Institutional Capacity

1. Develop specialised training programmes for law enforcement, prosecutors, and judges on investigating and prosecuting TFGBV, including digital evidence collection.

2. Establish online reporting mechanisms allowing victims to report cybercrimes securely and submit digital evidence.

3. Create multi-stakeholder technical groups or coordination mechanisms bringing together government, law enforcement, tech companies, and civil society.

4. Develop digital platforms for case tracking and data collection on TFGBV to enable evidence-based policymaking.

4.3 Provide support to Survivors

Eastern Partnership countries should strengthen survivor-centred responses to TFGBV through the development of accessible and secure digital response mechanisms, including safe online reporting channels, trauma-informed digital interfaces, and reliable referral pathways to specialised support services. Particular attention should be given to accessibility for young women, women in rural and remote areas, women with disabilities, and LGBTQI+ persons. In this context, EU engagement can play a catalytic role by supporting the institutionalisation and scaling-up of innovative digital tools piloted by civil society and international partners, thereby enhancing trust, accessibility, and the overall effectiveness of national protection systems.

1. Ensure holistic support services for TFGBV survivors, including psychological counselling, legal aid, and online safety assistance.

2. Require immediate notification to victims when perpetrators subject to protection orders are released from custody.

3. Develop targeted support for particularly vulnerable groups, including women journalists, human rights defenders, and women from minorities.

4.4 Increase Prevention and Awareness

1. Integrate digital citizenship and online safety education into school curricula at all levels.
2. Conduct public awareness campaigns on TFGBV, challenging norms that trivialise online violence.
3. Encourage media self-regulation and industry initiatives to combat sexist content and victim-blaming narratives.
4. Support the development and dissemination of resources and toolkits for youth and survivors on ending online gender-based violence, adapting successful regional models such as UN Women's Youth Guide to End Online Gender-Based Violence developed by the 30 for 2030 Network in Asia-Pacific.[25]
5. Develop specific protection mechanisms for women in the public eye, including women journalists, politicians, human rights defenders, and activists, who are disproportionately exposed to TFGBV as a form of political intimidation and silencing.[26]
6. Recognise that experiences of violence discourage women from expressing themselves online and lead to self-censorship, withdrawal from digital spaces, and increased tolerance for violence. Prevention strategies must address these consequences as barriers to women's equal participation in public, political, and economic life.[27]

The lack of disaggregated and comparable data on technology-facilitated gender-based violence across the Eastern Partnership region limits evidence-based policymaking and accountability. Integrating TFGBV indicators into national GBV data systems, administrative records, and EU-supported monitoring frameworks would support more effective GAP III reporting, enhance comparability across countries, and enable the tracking of progress under EU Enlargement and Association commitments.

4.5 Develop Whole-of-Society Prevention Strategies

Effective prevention of TFGBV requires a coordinated whole-of-society approach that engages all stakeholders - governments, civil society, the education sector, the technology industry, media, and communities - in addressing the root causes of digital violence against women.[28]

State Actors and Gender Equality Mechanisms

State actors should raise awareness among relevant professionals on the magnitude, manifestations, and consequences of TFGBV. This includes encouraging a more proactive role of the education system in raising student and teacher awareness on TFGBV through digital literacy curricula that integrate gender perspectives.[29] National gender equality policies and programmes should explicitly address digital literacy and knowledge advancement among the general population to improve personal security while using digital and communication technologies.

[25] UN Women, *Repository of UN Women's Work on Technology-Facilitated Violence Against Women and Girls* (March 2025), pp. 10-11.
[26] UN Women ECA, *The Dark Side of Digitalization* (2023), p. 6; EIGE, *Tackling cyber violence against women and girls* (2024), p. 16.
[27] UN Women ECA, *The Dark Side of Digitalization* (2023), p. 5.
[28] UN Women ECA, *The Dark Side of Digitalization* (2023), p. 7.
[29] Ibid., p. 7.

Engaging Men and Boys

Prevention strategies should actively engage men and boys not only as allies in addressing TFGBV, but also as individuals who can be directly affected by harmful digital norms, online harassment, and the normalisation of violent or self-harming behaviours in online spaces. Such practices reinforce rigid and unequal gender norms and contribute to toxic digital cultures that harm all users. Education on equitable and non-violent masculinities, digital responsibility, and respectful online communication should therefore be integrated into school curricula, youth programmes, and public awareness campaigns[30], with the aim of fostering critical digital literacy, empathy, and accountability, and promoting safer and more inclusive digital environments for all.

Media Responsibility

Media outlets should improve their awareness and understanding of TFGBV, and journalistic standards and codes should be revised to include ethical considerations related to reporting on digital violence. The media has a responsibility to raise awareness about TFGBV and accurately report on cases rather than minimising or romanticising the actions or their impact on victims.[31]

Civil Society and Women's Rights Organisations

State actors, as well as international and regional organisations, should support civil society organisations to strengthen their capacities to fully understand and provide services for TFGBV, and include CSOs as key partners in the development of programmes, policies, and legislation. Sustainable funding for CSO service providers, outside of project-based funding, should be ensured to maintain continuity of support for survivors.[32]

Multistakeholder Coordination

At the national level, all stakeholders must strengthen their cooperation and coordination to achieve a robust multisectoral approach to prevent and respond to TFGBV. In countries where cybercrime police are mandated with investigating TFGBV, they should be more systematically integrated into multisectoral mechanisms, and their roles in responding to TFGBV should be clearly defined in bylaws or protocols.[33]

At the international level, EaP countries should engage in regional and bilateral knowledge exchanges to learn from other countries and establish more coordinated efforts. International coalitions and networks such as the Generation Equality Action Coalitions on Technology and Innovation for Gender Equality and on Gender-Based Violence, which share TFGBV as a common priority, and the Global Partnership for Action on Gender-Based Online Harassment and Abuse, can leverage their commitments to accelerate progress toward ending TFGBV.[34]

4.6 Digital Platform Accountability

Research confirms that Facebook and Instagram are the platforms most frequently reported as locations where women experience technology-facilitated violence, with every third woman who experienced TFGBV having had that experience on one of these two platforms.[35] The

[30] Ibid., p. 7.
[31] Ibid., p. 8.
[32] Ibid., p. 8.
[33] Ibid., p. 8.
[34] UN Women, *Repository of UN Women's Work on Technology-Facilitated Violence Against Women and Girls* (March 2025), p. 1; UN Women ECA, *The Dark Side of Digitalization* (2023), p. 7.
[35] UN Women ECA, *The Dark Side of Digitalization* (2023), Executive Summary, p. 4.

role of digital platforms is therefore central to any comprehensive strategy to address TFGBV in the Eastern Partnership region.

Current Platform Limitations

Despite the high incidence of gender-related cyber violence, there is limited provision in digital platforms' standards and trust and safety policies for keeping users safe from TFGBV.[36] A 2024 study by the European Institute for Gender Equality (EIGE) found that platform standards and policies make little reference to relevant human rights frameworks or important legislative advances in combating gender-based violence and cyber violence. Platforms do not apply a specific gender perspective in policy development, nor do they explicitly refer to women and girls' experiences of cyber violence, where gender is highlighted, it is often only within the context of hate speech.[37]

Furthermore, digital platforms do not have cyber violence data disaggregated by sex available for incident reporting, response, and follow-up practices. This lack of a gender-sensitive approach at the level of reporting, recording, and responding to different forms of violence online renders the scale of TFGBV largely invisible and contributes to obscuring its dynamics.[38]

Engage with Digital Platforms:

Digital Platforms should be urged to:

1. **Incorporate gender-sensitive approaches** into the creation of policies and moderation procedures, fostering a more inclusive environment and improving content moderation effectiveness.[39]

2. **Reference significant legislative frameworks** combating GBV and CVAWG, such as the Istanbul Convention, GREVIO General Recommendation No. 1, and EU Directive 2024/1385, when developing and reviewing trust and safety practices.

3. **Implement harmonised definitions** of the different forms of TFGBV, referring to established frameworks including EIGE's publications and the measurement framework developed in line with the EU Directive on combating violence against women and domestic violence.

4. **Design reporting systems** to permit the collection of sex-disaggregated and other relevant data, enabling accurate assessment of the prevalence and incidence of TFGBV.

5. **React promptly and respond swiftly** to reports of harmful content—for example, by immediately suspending potential offenders' profiles and escalating cases to law enforcement where appropriate.

6. **Facilitate cross-platform reporting** recognising that violence crosses platform boundaries, enabling users to report TFGBV that happens outside a platform's immediate scope.

7. **Enhance cooperation with law enforcement** to improve response time to cases of TFGBV and more rapidly lock or remove offenders' accounts.[40]

[36] European Institute for Gender Equality (EIGE), *Tackling cyber violence against women and girls: The role of digital platforms* (Luxembourg: Publications Office of the European Union, 2024), p. 5.
[37] Ibid., p. 10.
[38] Ibid., p. 5.
[39] Ibid., p. 16.
[40] Ibid., pp. 16-17.

Regulatory Framework

The EU Digital Services Act (DSA), which became applicable in February 2024, places a range of legal obligations on online platforms including requirements related to content moderation and transparency reporting.[41] EaP countries, particularly EU candidate countries, should consider how domestic regulatory frameworks can align with DSA principles to ensure platform accountability. Multi-stakeholder technical groups or coordination mechanisms bringing together government, law enforcement, technology companies, and civil society, such as Moldova's Technical Group of Experts on TFGBV, provide a model for institutionalising platform engagement in addressing digital violence.

International mechanisms such as StopNCII provide practical tools for cross-platform cooperation in addressing non-consensual intimate image abuse, offering victims the ability to create digital fingerprints (hashes) of intimate images that platforms can use to detect and remove matching content.[42] EaP countries should encourage platforms operating in their jurisdictions to participate in such mechanisms and provide information to survivors about available tools and resources.

5. Conclusion

Technology-facilitated gender-based violence represents a rapidly evolving challenge that requires urgent, comprehensive responses. The adoption of EU Directive 2024/1385 provides a clear framework and benchmark for EaP countries to strengthen their legal and institutional frameworks.

Moldova's comprehensive legislative reforms offer a model for the region, demonstrating how to criminalise digital violence while building institutional capacity for implementation. Ukraine continues to build capacity despite extraordinary challenges, while Georgia, Armenia, and Azerbaijan are making incremental progress with international support.

For EU candidate countries in particular, alignment with Directive 2024/1385 is both a political imperative and an opportunity to enhance protection for women and girls in the digital age. The Eastern Partnership Working Group on Gender Equality has a vital role in facilitating exchange of good practices and supporting coordinated progress across the region.

Critically, research confirms that women rarely report cases of TFGBV to police (7.1%) or other institutions, with even lower rates of reporting to non-governmental organisations (2.5%). The primary reasons for non-reporting are the belief that nothing will be done, lack of trust in institutions, fear that confidentiality will not be respected, and fear of being blamed for the experience.[43] Building effective responses to TFGBV therefore requires not only strengthening legislative and institutional frameworks but also addressing the barriers that prevent survivors from seeking help. A high proportion of women (70.4%) want stronger accountability and responsibility from companies that own internet platforms and apps, more effective protection from institutions (66.5%), and more awareness raising to empower women to prevent, report, or counter TFGBV (69.7%).[44] These findings should guide EaP policy priorities and EU engagement strategies.

Addressing technology-facilitated gender-based violence is no longer a peripheral digital safety concern but a core gender equality, rule of law, and democratic governance priority for the Eastern Partnership. Coordinated EU action — grounded in GAP III, aligned with EU legal

[41] Ibid., p. 8.
[42] Ibid., p. 13.
[43] UN Women ECA, *The Dark Side of Digitalization* (2023), Executive Summary, p. 5.
[44] Ibid., p. 5.

standards, and embedded in Enlargement and Association processes — can support EaP partners in developing comprehensive, survivor-centred, and future-proof responses to digital violence against women and girls.