COFEM

Governing Technology-Facilitated Gender-Based Violence

Policy Brief:Strengthening Democratic Governance and Accountability

Key Points

Technology-facilitated gender-based violence is driving women out of public life. UN Women data from 2025[1] show that 41% of women in public-facing roles self-censor on social media, while nearly one in five have scaled back their professional work to avoid abuse. Among women journalists the figure rises to 45%, up from 30% in 2020.

Reporting has risen; accountability has not. Reports to police by women journalists doubled between 2020 and 2025.[2] Yet laws protecting women from cyber harassment exist in only about a third of economies, and few governments publish data on investigations, prosecutions or content removals.[3]

The dominant online safety framing puts the burden in the wrong place. It asks women to protect themselves while leaving action by platforms and institutions largely voluntary. TFGBV is better understood as a question of democratic governance because it determines who can participate in public life safely and visibly.

States already have obligations. CEDAW requires states to eliminate discrimination against women in political and public life, and the due diligence standard applies whether perpetrators are individuals or organised online networks.

This brief supports policymakers to address an institutional gap: which bod(ies) are answerable for outcomes, and to whom.

Introduction

Technology-facilitated gender-based violence (TFGBV) refers to violence committed through digital technologies that causes physical, sexual, psychological, social, political or economic harm.[4] Over the past few years, several regional bodies have strengthened the international frameworks to address TFGBV, such as:

In 2021, the Council of Europe's monitoring body interpreted the Istanbul Convention as applying fully to the digital dimension of violence against women (VAW).[5]

In 2022, the African Commission on Human and Peoples' Rights followed with a dedicated resolution on digital VAW in 2022.[6]

In 2024, the European Union criminalised four forms of online VAW, namely: cyber stalking, cyber harassment, cyber incitement to violence or hatred and non-consensual sharing of intimate or manipulated images and videos, including deep fakes.[7]

However, less progress has been made in determining who is responsible for addressing TFGBV.[8] Governmental institutions often distribute responsibility across institutions, with no single body accountable for outcomes. For example, police receive complaints but frequently lack the specialist skills needed to investigate technology-facilitated abuse. Communications regulators may oversee traditional media, while having little authority over platforms and recommender systems. Ministries responsible for gender equality often lead policy development without holding the regulatory power needed to translate policy into practice. As much as governments are working to address TFGBV, responsibilities remain fragmented and decentralised.[9]

This brief is intended for policymakers working in national governments and multilateral institutions, with particular attention to Global Majority contexts where constrained institutional capacity and inadequate criminal provisions carry risk of misuse. The brief starts with a short review of the current evidence on the nature and consequences of TFGBV and then examines the strengths and limitations of the principal regulatory approaches currently in use. Next, the brief reframes TFGBV from a lens of online safety to one of democratic governance. The brief concludes with recommendations for accountable institutions to prevent abuse before it happens.

What the evidence establishes

The prevalence of TFGBV is well documented, but questions remain about what those patterns of abuse mean for democratic participation, institutional accountability and public policy. A 2025 UN Women study found that 41% of women in public-facing roles self-censor on social media, and that nearly one in five have scaled back their professional work to avoid abuse. Among women journalists and media workers the figure rises to 45%, up from 30% in 2020, and roughly one fifth report self-censoring in their work itself. The health consequences are substantial, with almost a quarter diagnosed with or treated for anxiety or depression connected to the abuse, and 13% for post-traumatic stress disorder.[10] None of this appears in crime statistics, and neither does what follows it: the investigation not pursued, the candidacy not declared, and the account quietly closed.

In Uganda's 2021 election, men actually drew more negative social media comments overall. What differed was content: 18% of women's accounts were hit with sexualised abuse, more than double the 8% for men.[11] Kenya told a similar story a year later, where women candidates were attacked on social media for their appearance, sexuality, age and party affiliation.[12] The Inter-Parliamentary Union has tracked these same patterns in legislatures since 2016, with its most recent Asia-Pacific study finding that 60% of women parliamentarians experienced hate speech, disinformation, image-based abuse or doxxing.[13] Because this abuse rises predictably around elections, institutions can anticipate and plan for this risk.

Notably, more women report abuse through formal channels today than five years ago. Police reports among women journalists doubled between 2020 (11%) and 2025 (22%), while the proportion pursuing legal action increased from 8 to 14%.[14] Yet, only a third of countries have formal mechanisms for content removal, prosecutions/ verdicts and legal protection against cyber harassment.[15] The result is a significant accountability gap. Women report abuse in growing numbers, but few of those reports lead to investigation, removal, or legal consequence.

Four regulatory models and what they deliver

Governments have responded to TFGBV in different ways. In practice, four broad approaches have emerged. Few countries rely on only one of them, and the strongest responses tend to combine elements of several models. Each addresses a different aspect of the problem and brings its own strengths, limitations and implementation challenges.

1. Criminal regulation

Criminal regulation is the most common response to TFGBV and the one most likely to be misapplied. The European Union's 2024 Directive on combating violence against women requires Member States to criminalise cyber stalking, cyber harassment, cyber incitement to violence or hatred, and the non-consensual sharing of intimate or manipulated material. The directive also covers sexually explicit material that falsely appears authentic, which begins to address the harms of generative AI.

The problems arise after the offence is on the statute book.[16] For instance, Egypt's Maadi Misdemeanour Court arrested and sentenced Amal Fathy to two years' imprisonment under "false news" and public decency provisions after posting a video criticising the authorities' failure to protect her and other women from sexual harassment.[17] Legislation therefore needs to name the offence precisely, rather than relying on broad, catch-all provisions that can be turned against survivors themselves.[18] Much of what determines whether prosecutions succeed lies in the procedural detail behind the offence, the rules for preserving digital evidence, compelling platform disclosure and protecting survivor anonymity.

2. Administrative regulation

A second approach relies on administrative rather than criminal enforcement. Instead of prosecution, an independent regulator oversees compliance through actions such as content removal and imposing civil penalties. Australia's eSafety Commissioner represents one of the most developed examples of this model. Operating under the Online Safety Act 2021, the Commissioner combines a central reporting mechanism with statutory removal powers, civil penalties and publicly available performance reporting.[19] Approximately 90 per cent of removal requests issued to platforms have resulted in the removal of some or all reported material.[20] For a woman whose intimate images are circulating, that speed matters more than any eventual conviction would.[21] The model has two clear limits.[22] First, its success is highly implementation-dependent since much rests on whether there is a well-publicised and well-resourced reporting channel behind it. Second, removal addresses the immediate harm but not accountability: the image comes down, but the perpetrator faces no penalty, deterrent, or record.

3. Systemic risk regulation

Systemic risk regulation is the only model that addresses how a platform's own design: its recommendation systems, ranking, and virality mechanics. It asks instead whether the architecture of a platform contributes to foreseeable harm, and what the company owes in response. Instead of asking whether a particular post should come down, it asks whether the architecture of a platform contributes to foreseeable harm and what the company owes in response. For instance, The European Union's Digital Services Act (2022) mandates large online platforms to identify, assess and mitigate systemic risks arising from the design and operation of their services, including recommendation algorithms and advertising models, with gender-based violence (GBV) explicitly named among the risks platforms must address.[23] Design and commercial incentive shape the visibility of abusive content as much as by user behaviour. It also produces something the other models lack, accountability for the platform's own design choices, not just individual pieces of content.

Supervising systemic risk demands technical skills inside the companies themselves, which creates an obvious tension in asking firms to assess their own risks.[24] For the model to work in practice, risk assessments would need to disaggregate impacts by group. The harder problem is capacity, which most smaller states cannot solve alone. Regional cooperation is the more realistic route, and while the African Union's Malabo Convention does not establish a framework for platform supervision, it demonstrates that continental cooperation on cybersecurity and digital governance is achievable through a binding continental instrument that obliges States Parties to harmonise their domestic legislation on cybersecurity, cybercrime and personal data protection. Its slow ratification is caution as much as proof, with only 17 of 55 member States bound as of June 2025 but demonstrates that African States can negotiate binding continental standards on digital governance and hold each other to them.[25]

4. Electoral regulation

Electoral regulation treats coordinated abuse of women candidates and elected representatives as a threat to democratic competition rather than only as a criminal matter or a platform problem. Latin America has been at the forefront of developing this model.[26] Mexico's 2020 reforms amended several federal laws at once, establishing a legal definition of political VAW on grounds of gender, licensing the National Electoral Institute authority to investigate and sanction it, and authorizing electoral institutions to enable women's equal political participation.[27] Electoral bodies move faster than criminal courts and can deregister candidates, restrict access to public funding, require corrective action by parties and maintain registers of sanctioned individuals, sanctions that bite precisely because they touch political participation itself.[28] However, electoral management bodies are often under-resourced and operate in contested environments, so independence is essential in order to apply sanctions consistently. Anonymous networks, foreign actors and platform amplification lie largely beyond the reach of electoral bodies.[29] Measures designed to protect women from gendered political violence must also not be drafted so broadly that they shield officials from legitimate scrutiny.[30] What would make the model function rather than merely exist is a combination of adequately resourced and independent electoral bodies, formal cooperation with platforms and other authorities to reach actors beyond electoral bodies' own jurisdiction, and safeguards that prevent these powers from being used to shield officials from legitimate criticism.[31]

From online safety to democratic governance

The current policy response to TFGBV is often framed in terms of online safety, with emphasis on helping individuals protect themselves through stronger privacy settings, improved digital security, content reporting mechanisms, and faster takedowns. These interventions are important and should remain part of any comprehensive response. On their own, however, survivors face the heavy burden of responsibility while largely relying on voluntary action from the institutions and companies that have the greatest capacity to reduce harm at scale.

Consequently, TFGBV should be understood as a question of democratic governance. The issue extends beyond personal safety because it shapes who can safely and visibly participate in public life. That shift in perspective has implications for how governments understand both their obligations and the institutions responsible for meeting them. International human rights law already provides part of this foundation. States have obligations under CEDAW, for example, to eliminate discrimination against women in political and public life. These obligations remain in effect whether the immediate perpetrators are private individuals or organised online networks. CEDAW General Recommendation No. 35 (2017) on GBV against women, updating general recommendation No. 19 (1992), makes clear that these due diligence obligations extend to TFGBV and require states to prevent, investigate and respond to such harm.[32] Meeting that obligation requires looking past individual perpetrators. Coordinated harassment campaigns, algorithmic amplification, and the rapid circulation of abusive content don't emerge from isolated actions; rather, they're shaped by the design and operation of digital platforms and the regulatory choices that influence how information spreads.

Finally, the consequences of TFGBV extend well beyond those directly targeted. Democratic institutions face the collective consequences when journalists abandon investigations, candidates choose not to stand for election or women withdraw from public life. Public debate narrows and citizens face diminished e quality of information. These outcomes fall squarely within the mandates of governments, electoral authorities, legislatures and communications regulators. Viewing TFGBV through a governance lens therefore broadens both responsibility and the range of available policy responses. Criminal law, electoral law, platform regulation, administrative oversight, public investment and institutional accountability all have roles to play in creating an environment in which women can participate.

Guiding principles for an effective democratic governance ecosystem

The recommendations below are organised by the institutions best placed to act. No single intervention, institution, law or regulator can address TFGBV alone. Effective governance requires legislators, regulators, electoral bodies and funders to pull in the same direction, each covering ground the others can't reach.

Legislators and justice institutions

Harm-specific drafting.

Laws define clear, specific forms of harassment rather than categories of speech – criminalising conduct such as non-consensual intimate image sharing, credible threats and coordinated intimidation – while avoiding vague offences that can be used against journalists, activists or political opponents. Safeguards for legitimate political expression are explicit.

Enforcement infrastructure.

New offenses are paired with clear rules on digital evidence, platform disclosure, survivor protection and cross-border cooperation.

Future-proof definitions.

Legal definitions explicitly encompass synthetic and AI-generated content so that reforms remain effective as technologies evolve, rather than requiring continual legislative amendment.

Transparent measurement.

Governments routinely publish data on reports, investigations, prosecutions and outcomes so that both effectiveness and potential misuse can be monitored over time.

Regulators

Systemic focus.

Regulatory frameworks require platforms to identify, assess and mitigate the ways in which recommender systems, design choices and business models contribute to TFGBV.

Regional cooperation.

Where appropriate, regional approaches support collective and long-term supervisory expertise, offering a realistic and sustainable model for oversight.

Transparent reporting.

Platforms measure impact through transparent reporting, independent audits, and publicly available performance data.

Independent scrutiny.

Researchers and civil society have meaningful access to platform data to independently verify regulatory claims and platform risk assessments.

Governments and donors

Response as public infrastructure.

Women's organisations, legal services, digital security providers and psychosocial support services perform essential public functions through sustainable, multi-year investment.

Evidence base.

Governments routinely collect and publish prevalence and administrative data on TFGBV, including reporting, investigations, enforcement actions, and outcomes.

Implementation capacity.

Governments invest in the people and resources needed to enforce new laws and regulatory frameworks, strengthening the capacity of the institutions responsible for running them.

Multilateral cooperation.

Rather than creating new mechanisms, governments strengthen cooperation through existing regional and international frameworks to address cross-border challenges such as synthetic media, platform governance and regulatory standards.

Researchers and monitoring bodies

Comparable evidence.

Consistent TFGBV measures, including prevalence, self-censorship, reporting, enforcement outcomes, and time to resolution, enable governments to compare approaches, evaluate reforms and identify emerging trends across jurisdictions.

Balanced monitoring.

Research gives equal attention to implementation and prevalence, examining how laws and regulatory frameworks operate in practice, including patterns of investigation, prosecution, enforcement, and potential misuse.

Conclusion

Most states still treat TFGBV as a problem of harmful content. Yet the evidence points to a problem of democratic governance that determines who can participate in public life, on what terms, and at what cost. Rather than creating new offences or strengthening platform regulation, states can build institutions capable of preventing harm, enforcing rights, and holding powerful actors to account. Laws matter, but so does regulatory capacity, institutional coordination, sustainable investment, survivor-centred implementation, and independent oversight.

What we are asking governments to measure is whether women can participate in public life, online and offline, without paying for it in fear, harassment, or silence.

Suggested Citation

Joy Watson. Coalition of Feminists for Social Change. Governing Technology-Facilitated Gender-Based Violence: Strengthening Democratic Governance and Accountability (2026)

References

[1] Posetti, J., Hellmueller, L., Williams, K., Renaud, P., Aboulez, N. and Shabbir, N., 2025. Tipping point: The chilling escalation of online violence against women in the public sphere. New York: UN Women. Available at: https://www.unwomen.org/sites/default/files/2025-12/tipping-point-the-chilling-escalation-of-violence-against-women-in-the-public-sphere-in-the-age-of-ai-en.pdf

[2] Posetti, J., Hellmueller, L., Williams, K., Renaud, P., Aboulez, N. and Shabbir, N., 2025. Tipping point: The chilling escalation of online violence against women in the public sphere. New York: UN Women.

[3] Affoum, N.R.M., Santagostino Recavarren, I.M., Vohra, N. and Wodon, Q., 2023. Protecting Women and Girls from Cyber Harassment: A Global Assessment of Existing Laws. Global Indicators Briefs No. 18. Washington, DC: World Bank. Available at: https://openknowledge.worldbank.org/server/api/core/bitstreams/61bf29ba-c5c8-4859-9c66-f5d4b139a745/content

[4] UN Women, 2022. Expert Group Meeting Report: Technology-facilitated violence against women: Towards a common definition, 15–16 November 2022, New York. Available at: https://www.unwomen.org/sites/default/files/2023-03/Expert-Group-Meeting-report-Technology-facilitated-violence-against-women-en.pdf

[5] Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO), 2021. General Recommendation No. 1 on the digital dimension of violence against women, adopted 20 October 2021. Strasbourg: Council of Europe. Available at: https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women-en/1680a49147

[6] African Commission on Human and Peoples' Rights, 2022. Resolution on the Protection of Women Against Digital Violence in Africa, ACHPR/Res. 522 (LXXII) 2022, adopted at the 72nd Ordinary Session, 19 July to 2 August 2022. Available at: https://achpr.au.int/en/adopted-resolutions/522-resolution-protection-women-against-digital-violence-africa-achpr

[7] Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence, Official Journal of the European Union, L 2024/1385, 24 May 2024.

[8] UK Foreign, Commonwealth & Development Office, 2023. Technology-Facilitated Gender-Based Violence: Preliminary Landscape Analysis.

[9] UN Women, SVRI, APC & Global Partnership for Action on Gender-Based Online Abuse and Harassment, 2024. Technology-facilitated gender-based violence: Developing a shared research agenda.

[10] Posetti J, Hellmueller L, Williams K, Renaud P, Aboulez N and Shabbir N 2025.

[11] Pollicy, 2021. Amplified Abuse: Report on Online Violence Against Women in the 2021 General Elections. Kampala: Pollicy. Available at: https://pollicy.org/wp-content/uploads/2022/08/Amplified-Abuse-Report-on-online-violence-Against-women-in-the-2021-general-elections.pdf

[12] Pollicy (2023). Byte Bullies: Online Violence Against Women in Politics in the 2022 Kenya General Elections. Kampala: Pollicy. Available at: https://pollicy.org/wp-content/uploads/2023/05/Byte_Bullies_report.pdf.

[13] Inter-Parliamentary Union (IPU), Commonwealth Parliamentary Association (CPA) and ASEAN Inter-Parliamentary Assembly (AIPA), 2025. Sexism, Harassment and Violence Against Women in Parliaments in the Asia-Pacific Region. Geneva: IPU.

[14] Posetti J, Hellmueller L, Williams K, Renaud P, Aboulez N and Shabbir N 2025.

[15] Affoum, N.R.M.; Santagostino Recavarren, I.M.; Vohra, N.; Wodon, Q 2023.

[16] Steinmetz, K.F., Schaefer, B.P., McCarthy, A.L., Brewer, C.G. and Kurtz, D.L., 2024. Exploring Cybercrime Capabilities: Variations Among Cybercrime Investigative Units. Criminal Justice Policy Review, 35(4), pp.194–215.

[17] International Commission of Jurists, 2018. Egypt: Conviction of human rights defender Amal Fathy for social media criticism must not stand, 20 December 2018. Geneva: ICJ. Available at: https://www.icj.org/egypt-conviction-of-human-rights-defender-amal-fathy-for-social-media-criticism-must-not-stand/

[18] Derechos Digitales, 2022. When Protection Becomes an Excuse for Criminalisation: Gender Considerations on Cybercrime Frameworks. Santiago: Derechos Digitales. Available at: https://www.derechosdigitales.org/wp-content/uploads/gender_considerations_on_cybercrime.pdf

[19] Parliament of Australia, 2021. Online Safety Act 2021 (Cth). Available at: https://www.legislation.gov.au/C2021A00076/latest/text

[20] eSafety Commissioner, 2024. Insights from eSafety's image-based abuse reporting and removal scheme. Canberra: Australian Government. Available at: https://www.esafety.gov.au/research/insights-from-esafetys-image-based-abuse-reporting-and-removal-scheme

[21] eSafety Commissioner, 2024. Insights from eSafety's Image-Based Abuse Reporting and Removal Scheme. Sydney: eSafety Commissioner.

[22] Media Defence, 2024. Module 7: Cybercrimes — Summary Modules on Litigating Digital Rights and Freedom of Expression. London: Media Defence. Available at: https://www.mediadefence.org/ereader/wp-content/uploads/sites/2/2022/12/Module-7-Cybercrimes-2024.pdf

[23] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act), Official Journal of the European Union, L 277, 27 October 2022, Articles 34–35; see also Martins, P., 2024. How Can Impact Assessments Improve Protection from TFGBV? Waterloo, ON: Centre for International Governance Innovation.

[24] Kaminski, M.E., 2023. The Developing Law of AI: A Turn to Risk Regulation. The Digital Social Contract: A Lawfare Paper Series; University of Colorado Law Legal Studies Research Paper No. 24-5.

[25] African Union, 2014. African Union Convention on Cyber Security and Personal Data Protection (Malabo Convention), adopted 27 June 2014, entered into force 8 June 2023. Available at: https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

[26] Restrepo Sanín, J., 2021. Latin America Leads the Way in Fighting Violence and Harassment against Women in Politics. European Journal of Politics and Gender.

[27] Corral Limas, L.G., Morales Corral, A.Y. and Lozano Sandoval, V.O., 2020. Gender-Based Political Violence in Mexico: A Complex Assignment. Saudi Journal of Humanities and Social Sciences, 5(8). See also Ley General de Acceso de las Mujeres a una Vida Libre de Violencia and Ley General de Instituciones y Procedimientos Electorales, as amended 13 April 2020.

[28] Corral Limas, L.G., Morales Corral, A.Y. and Lozano Sandoval, V.O., 2020.

[29] United Nations Development Programme (UNDP) and Inter-Parliamentary Union (IPU), 2026. Addressing Violence Against Women in Politics: Institutional Responses and Good Practices by Parliaments. New York: UNDP.

[30] UN Women, 2018. Violence against Women in Politics: Expert Group Meeting Report and Recommendations. New York: UN Women.

[31] Michalko, J. and Jiménez Thomas Rodriguez, D., 2026. Online Violence Against Women in Politics: What Shapes Political Party Responses to Technology-Facilitated Gender-Based Violence? London: ALIGN/ODI.

[32] Committee on the Elimination of Discrimination against Women, 2017. General recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19, CEDAW/C/GC/35, adopted 14 July 2017, paras 24(b) and 26.