

Credit: FG Trade Latin / iStock

Technology-facilitated gender-based violence: Policy recommendations for accelerating domestication and implementation of the SADC Model Law

June 2026

Equality Now

A just world for all women and girls

SADC Parliamentary Forum
Forum Parlementaire
Fórum Parlamentar

Equality Now
A just world for all women and girls

About Equality Now

Equality Now is a worldwide human rights organisation dedicated to securing the legal and systemic change needed to end discrimination against all women and girls, everywhere in the world. Since its inception in 1992, it has played a role in reforming 130 discriminatory laws globally, positively impacting the lives of hundreds of millions of women and girls, their communities and nations, both now and for generations to come.

Working with partners at national, regional, and global levels, Equality Now draws on deep legal expertise and a diverse range of social, political, and cultural perspectives to continue to lead the way in steering, shaping, and driving the change needed to achieve enduring gender equality, to the benefit of all.

SADC
Parliamentary Forum
Forum Parlementaire
Fórum Parlamentar

About the Southern African Development Community Parliamentary Forum (SADC PF)

The SADC Parliamentary Forum (SADC PF) is established under Article 9(2) of the SADC Treaty, and it forms part of the institutional framework of the Southern African Development Community (SADC). Its main objective is to promote inter-parliamentary initiatives on common objectives to advance democracy, the rule of law, and human rights in the region. Guided by its Strategic Plan (2024-2028), it is mandated to adopt Model Laws that serve as guiding benchmarks for Members of Parliament (MPs) in Southern Africa and beyond. The Forum currently comprises 15 Member Parliaments, with representation from over 3,500 MPs.

Acknowledgements

This report is a joint publication by the SADC PF and Equality Now, made possible through the collective efforts of a team of individuals around the world. In particular, we acknowledge the contribution of the SADC PF team: Her Excellency Boemo Sekgoma (SADC PF Secretary General), and the representatives of the SADC PF Secretariat, including Krishna Seegobin (Barrister and Legal and Policy Advisor), Sheuneni Kurasha (Director of Programmes), and Equality Now's team: Sally Ncube (Regional Representative - Southern Africa), Tsitsi Matekaire (Director, Regions), Amanda Manyame (Director, Securing Digital Rights) and the communications team. We also acknowledge the contribution of Tatenda Zvogbo, a consultant who conducted the research for this report, providing information on the situation of technology-facilitated gender-based violence (TFGBV) and legal and policy frameworks across the SADC member states.

Table of contents

1. Executive summary **5**
- Methodology 5
- Headline findings 6
- Key recommendations 6
- Regional-level (SADC Parliamentary Forum and SADC Secretariat) 6
- National governments (Parliaments and Ministries of Justice) 7
- Regulators and law enforcement 7
- Civil society and service providers 7

2. Introduction **8**

3. The SADC Model Law on gender-based violence: An overview **9**

4. Findings **11**
- 4.1 Half-mast analysis 12
  - 4.1.1 Preliminary provisions: Definitions and scope 12
  - 4.1.2 Human rights-based approach and policy direction 13
  - 4.1.3 Access to justice and procedural protections 14
  - 4.1.4 Prohibition of gender-based violence and attendant procedures 14
  - 4.1.5 Early and effective response mechanisms and referral systems 15
  - 4.1.6 Prevention, protection, support and intervention measures 15
  - 4.1.7 Data, capacity, public awareness, monitoring and evaluation 16
  - 4.1.8 Enforcement, compliance and regulatory mechanisms 16

5. Illustrative case studies **17**

6. Good practices in SADC **18**

7. Recommendations **19**
- Regional level – SADC-PF and Secretariat 19
- National level – Parliaments and Ministries of Justice 19
- Regulators and law enforcement 19
- Civil society and service providers 19

Conclusion **20**

Annexure 1: 16-Country domestication snapshot **21**

Endnotes **22**

1. Executive summary

Technology-facilitated gender-based violence (TFGBV) is an escalating challenge that undermines gender equality, digital safety, and the rights of women and girls in Southern Africa. Although most Southern African Development Community (SADC) member states have enacted laws and adopted policies on gender-based and sexual violence, cybercrime, data protection, and trafficking in persons, among others, their implementation and harmonisation remain uneven, leaving gaps in protection against the growing and emerging forms of TFGBV. Weak enforcement, fragmented data, and limited survivor-centred digital safety systems leave significant gaps between legal and policy progress and the lived realities of survivors.

Recent regional analyses show that Southern Africa, despite having the continent's highest internet penetration, faces rising levels of online abuse.[1] Women and girls, along with other marginalised groups, are disproportionately affected by TFGBV, including sexual exploitation and abuse, coordinated harassment, threats, and disinformation campaigns. Women and young people in the public space, including politicians, journalists, activists and human rights defenders, are particularly vulnerable to cyberstalking, sexual coercion and extortion, and image-based sexual exploitation, abuses that often combine sexualised violence with efforts to undermine their credibility or public presence. Across the board, many survivors face significant barriers to reporting or obtaining redress, as TFGBV cases are not always recognised as violations or crimes, digital evidence is frequently poorly preserved or inadequately handled, perpetrators operate across jurisdictions, and online service providers are rarely compelled to cooperate effectively with law enforcement authorities. Due to the prevalence of TFGBV, the African Union (AU) adopted the AU Convention on Ending Violence Against Women and Girls in February 2025, which expressly covers all forms of violence, including those in cyberspace[2], thus giving credence to the rationale for the SADC Model Law on Gender-Based Violence for the Southern African region.

This report examines how the SADC Model Law on Gender-Based Violence can be leveraged to strengthen national legal, institutional, and regulatory frameworks for responding to TFGBV. It provides legal and policy recommendations for member states and technology companies towards an improved response, aligned with their responsibilities and obligations under international and regional human rights law and standards.[3]

Methodology

The report was developed based on research commissioned by Equality Now and the SADC PF, which examined and analysed laws and policies relevant to TFGBV across the Southern African region, as well as the SADC Model Law on Gender-Based Violence. It applied a half-mast lens, an approach that assesses what is working, where gaps remain, and what concrete actions can close the divide across 8 thematic pillars, namely:

1. Preliminary provisions: definitions and scope;
2. Human rights-based approach and policy direction;
3. Access to justice and procedural protections;
4. Prohibition of GBV and attendant procedures;
5. Early and effective response mechanisms and referral systems;
6. Prevention, protection, support, and intervention measures;
7. Data, capacity, public awareness, and monitoring;
8. Enforcement, compliance, and regulatory mechanisms.

The assessment of law, policy, and practice applied four interlinked evidence layers:

1. **Framework mapping** – reviewing the SADC Model Law and other regional and global legal instruments relevant to GBV and digital rights and safety.
2. **National scan** – analysing constitutional, legislative, and policy frameworks in all 16 SADC countries.
3. **Jurisprudence and oversight** – reviewing case law, regulator actions, and parliamentary proceedings in targeted countries.
4. **Validation** – triangulating national findings through consultations with regional experts and practitioners.

Headline findings

Working	Gaps
11 of 16 countries have enacted cybercrime or electronic-evidence laws; five explicitly include TFGBV offences.	Many countries lack NCII (non-consensual intimate-image) and sexual extortion and coercion offences.
All Member States have trafficking laws; several mention online recruitment.	Few explicitly recognise technology as a means of facilitating trafficking.
Domestic-violence laws in Botswana, Lesotho, and Zimbabwe extend to electronic contact.	No uniform judicial guidance for preservation or takedown of online content.
Eleven countries have data-protection frameworks; regulators in Botswana, Seychelles and South Africa are operational.	Few regulators handle survivor privacy or TFGBV-related complaints.
National GBV policies increasingly recognise digital harms.	Implementation remains underfunded; no state has a dedicated TFGBV mechanism or data system.

Key recommendations

Addressing TFGBV requires a coordinated and multi-level response that bridges the gap between existing gender-based violence frameworks and the realities of harm in digital spaces. The recommendations outlined below call for strengthened legal and policy frameworks, improved enforcement and institutional capacity and survivor-centred services that respond effectively to online abuse and exploitation. They also emphasise the importance of regional cooperation, better data and monitoring and clear accountability mechanisms for digital platforms. Together, these measures aim to ensure that responses to TFGBV are comprehensive, rights-based and capable of protecting women and girls across both online and offline environments.

The report recommends a multi-level, coordinated response that combines legal and policy reform, stronger enforcement, survivor-centred services, regional cooperation, and platform accountability to close the gap between existing gender-based-violence frameworks and the realities of digital harm.

Regional-level (SADC Parliamentary Forum and SADC Secretariat)

- Develop a regional amendment or guidance framework to strengthen the response to TFGBV under the SADC Model Law on GBV.
- Establish a regional TFGBV observatory to track data trends and policy progress.
- Create regional cooperation mechanisms for digital evidence sharing, cross-border investigations and content takedown.
- Facilitate regular parliamentary engagement and peer learning on TFGBV and technology-enabled trafficking.

National governments (Parliaments and Ministries of Justice)

- Strengthen and harmonise national laws by updating cybercrime, GBV and data protection legislation to explicitly cover TFGBV offences, for instance, non-consensual intimate image sharing, online grooming and sexual coercion and extortion.
- Amend trafficking and GBV laws to recognise ICTs as tools used for exploitation and recruitment.
- Introduce rapid protection mechanisms, including electronic protection orders and clear digital evidence procedures.
- Build judicial and prosecutorial capacity through specialised training on TFGBV investigations and case management.

Regulators and law enforcement

- Establish trusted-flagger channels and cooperation agreements with online platforms to enable faster response to TFGBV content.
- Create 24/7 cybercrime hotlines or TFGBV focal points within police and prosecution services to support survivors.
- Develop clear notice-and-action procedures and regulatory guidance for platforms.
- Publish regular enforcement and transparency reports on TFGBV cases and digital content removal.

Civil society and service providers

- Expand survivor support services to include digital safety assistance, evidence preservation and support for removing harmful online content.
- Provide specialised legal and psychosocial services tailored to survivors of online abuse and exploitation.
- Lead public awareness campaigns on digital safety risks such as online grooming, sexual coercion and extortion and image-based abuse.

2. Introduction

The SADC Model Law on Gender-Based Violence was adopted by the 39th Plenary Assembly of the SADC Parliamentary Forum in 2016 in Eswatini to provide member states with a practical legislative yardstick for preventing, responding to, and eradicating gender-based violence (GBV). It translates regional and international human rights standards into model provisions that national policymakers can adapt. The **Model Law** is normative rather than binding - its full value can only be realised when member states domesticate its provisions through their own laws, policies, and implementation frameworks.

For the purpose of this report, TFGBV is defined as an act of violence perpetrated by one or more individuals that is committed, assisted, aggravated, and amplified in part or fully by the use of information and communication technologies or digital media, against a person based on their gender and/or sexual identity or by enforcing harmful gender norms. This definition is a mix of TFGBV definitions developed by UNFPA, NORC at the University of Chicago, and the International Center for Research on Women.[4] Taken together, this definition is comprehensive and captures the diverse forms, contexts, and harms associated with TFGBV across different digital environments and lived experiences. This definition is also in line with the definition of "cyberspace" in the AU Convention, which is "*a digital medium of communication and interaction of global or interconnected systems*".[5]

In Southern Africa, TFGBV manifests in pervasive and intersecting forms, including online harassment and threats, cyberstalking, non-consensual sharing of intimate images, tech-facilitated trafficking for sexual exploitation, sexual extortion and coercion, doxxing, impersonation, and the use of digital platforms to incite offline violence.[6] Women and girls in public life, such as journalists, activists, politicians, and human rights defenders, are particularly targeted, as are adolescent girls. These abuses are often compounded by limited digital literacy, unequal access to justice, cross-border perpetrators, and weak platform accountability, intensifying harm and silencing women's participation in public and civic spaces. Digital violence is no longer peripheral. It is a central form of harm.

In this report, TFGBV is understood as occurring within the continuum of GBV. In the experiences of survivors, online and offline abuses are not separate; they are profoundly interconnected and mutually reinforcing, with technology often amplifying existing patterns of gender-based violence. Limited digital literacy, combined with factors such as displacement due to changing climatic conditions and persistent poverty, creates fertile ground for sexual exploitation. Technology has enabled perpetrators to exploit these vulnerabilities, targeting women and girls in both rural and urban settings with false promises of better livelihoods.

Across Southern Africa, digital connectivity continues to expand, creating new spaces for both empowerment and abuse. By 2021, only about 22% of the total population in Sub-Saharan Africa used mobile internet, and women remain less likely than men to use it, which affects exposure, reporting, and access to help.[7] Recent data show that women in low- and middle-income countries are 15% less likely to use mobile internet than men.[8][9] This gap compounds existing inequalities and shapes how survivors experience and report online violence.

Several SADC member states are already aligning aspects of their domestic laws with the Model Law. For example, Lesotho's Counter Domestic Violence Act (2022) recognises technological abuse and provides for protection orders that restrict electronic contact.[10] South Africa has recently taken steps to strengthen its gender-based violence legal framework, including judicial and statutory reforms that effectively close legal gaps in how GBV crimes are prosecuted and addressed.[11] These developments show that domestication is both feasible and necessary, yet progress remains uneven, particularly in relation to digital-evidence procedures, survivor privacy, and cross-border cooperation.

The domestication of the Model Law, therefore, presents an opportunity to establish a coherent, survivor-centred response that covers all forms of TFGBV. By embedding clear definitions, ensuring access to justice and remedies, and strengthening institutional accountability, member states can build legal and policy systems that protect individuals, particularly women and girls, in both online and offline spaces.

> "Limited digital literacy, combined with factors such as displacement due to changing climatic conditions and persistent poverty, creates fertile ground for sexual exploitation. Technology has enabled perpetrators to exploit these vulnerabilities, targeting women and girls in both rural and urban settings with false promises of better livelihoods."

3. The SADC Model Law on gender-based violence: An overview

The SADC Model Law on Gender-Based Violence (SADC Model Law) establishes a comprehensive framework for the prevention, protection, and punishment of all forms of GBV, aligning national legislation with regional and international human rights standards. It provides a legislative guide for member states to strengthen laws, policies, and institutions addressing GBV in all its forms, including emerging manifestations such as technology-facilitated violence and technology-enabled trafficking.

The Model Law defines gender-based violence broadly to include physical, sexual, psychological, and economic harm. Section 6(3)(k) of the Model Law clarifies that GBV may include "online gender-based cybercrimes and bullying." This definition enables Member States to extend protection to survivors of online harassment, cyberstalking, image-based abuse, and coercive control perpetrated through digital platforms. It adopts a multisectoral and intersectional approach, recognising that effective GBV prevention and response require collaboration across the justice, Information and Communication Technology (ICT), law enforcement, education, and social welfare sectors. This approach supports comprehensive national strategies that integrate digital safety, survivor empowerment, and institutional accountability.

Summary of the provisions of the Model Law

Chapter	Focus	Key elements and provisions
Chapter 1: Preliminary provisions	Purpose, scope, and principles	Sets out the objectives of the Model Law; affirms state obligations to prevent, respond to, and eliminate GBV; establishes guiding principles, including survivor-centred, human rights-based, and gender-responsive approaches; defines key terms, including broad and inclusive definitions of GBV.
Chapter 2: Forms of gender-based violence	Substantive scope of GBV	Recognises multiple and intersecting forms of GBV, including physical, sexual, psychological, economic, and emotional violence, as well as harmful practices and emerging forms such as technology-facilitated GBV; acknowledges violence in both public and private spheres.
Chapter 3: Prevention of gender-based violence	Primary prevention measures	Requires states to adopt measures to prevent GBV, including public education, awareness-raising, gender-transformative programmes, engagement with men and boys, and integration of GBV prevention into education, media, and community structures.
Chapter 4: Protection of survivors	Survivor safety and protection	Provides for accessible and timely protection measures, including protection orders and safety planning; emphasises confidentiality, non-discrimination, and the best interests of survivors; includes provisions for children and persons with disabilities.

Chapter 5: Services and support for survivors	Survivor-centred services	Mandates comprehensive, coordinated services for survivors, including health care, psychosocial support, legal assistance, shelters, and economic empowerment; promotes referral pathways and multi-sectoral coordination.
Chapter 6: Criminalisation and legal remedies	Accountability and justice	Requires states to criminalise acts of GBV and ensure effective investigation, prosecution, and adjudication; provides for civil remedies and compensation; and discourages harmful practices, such as mandatory mediation or reconciliation, in GBV cases.
Chapter 7: Institutional frameworks and coordination	Governance and implementation	Establishes obligations for national coordination mechanisms; clarifies the roles of government institutions; and promotes multi-sectoral and multi-stakeholder collaboration to ensure the effective implementation of GBV laws and policies.
Chapter 8: Monitoring, evaluation, and data	Accountability and evidence	Requires collection, analysis, and publication of disaggregated data on GBV; promotes monitoring and evaluation of laws and policies; supports evidence-based decision-making and transparency.
Chapter 9: Funding and resources	Sustainability	Requires states to allocate adequate financial, human, and technical resources for GBV prevention and response; emphasises sustainable funding for services, institutions, and implementation mechanisms.
Chapter 10: Miscellaneous and transitional provisions	Alignment and implementation	Provides guidance on harmonising existing laws with the Model Law; includes transitional measures and timelines to support domestication and effective enforcement at the national level.

4. Findings

Across Southern Africa, the SADC Model Law has emerged as an important normative reference point, shaping national legal and policy reforms to strengthen protections for women and girls, including in digital and technology-mediated contexts. While levels of domestication vary, there is clear evidence of growing legal and policy momentum across the region.

Several SADC member states have enacted or updated legislation that aligns with the Model Law's intent, particularly regarding technology-facilitated forms of harm. South Africa, Botswana, Zimbabwe, and Mauritius have introduced cybercrime, data protection or TFGBV-relevant laws that reflect key principles of the Model Law, including recognition of non-physical forms of violence and the need for legal remedies in digital environments. In parallel, Namibia and Mozambique have advanced cybercrime and data protection bills that, if adopted, could further strengthen regional alignment.

Despite this progress, significant gaps remain. Definitions of technological abuse are inconsistent across jurisdictions, resulting in uneven protection for survivors. Existing frameworks, such as South Africa's Cybercrimes Act (2020) and Namibia's Combating of Domestic Violence Act (2022), provide partial coverage of online abuse. Almost all trafficking in persons laws do not explicitly address trafficking and exploitation facilitated through digital platforms. More broadly, many trafficking and cybercrime laws in the region continue to prioritise enforcement over survivor protection, with limited safeguards, weak remedies, and minimal obligations on digital platforms.

Implementation challenges further constrain impact. Technical capacity gaps, limited budgets, and insufficient institutional coordination continue to delay effective enforcement and undermine the transformative potential of these reforms. As a result, while the Model Law has clearly influenced the direction of legal change in Southern Africa, translating regional standards into comprehensive, survivor-centred, and enforceable domestic frameworks remains an ongoing challenge.

"While the Model Law on GBV has clearly influenced the direction of legal change in Southern Africa, translating regional standards into comprehensive, survivor-centred, and enforceable domestic frameworks remains an ongoing challenge".

4.1 Half-mast analysis

4.1.1 Preliminary provisions: Definitions and scope

Why this matters
Clear, inclusive definitions ensure that all forms of violence committed through any medium, including through the use of digital technology, are treated as GBV.

Progress (What is working)

- **South Africa:** The Cybercrimes Act 2020[12] defines and criminalises the disclosure of intimate images without consent.
- **Lesotho:** Counter Domestic Violence Act 2022[13] recognises "technological abuse" and supports electronic-contact bans.
- **Zimbabwe:** Cyber and Data Protection Act 2021[14] creates an explicit non-consensual intimate images offence.
- **Mauritius:** The Cybersecurity and Cybercrime Act 2021[15] creates a list of meaningful offences, including misuse of fake profiles, cyber extortion, and revenge pornography, which are potentially GBV-related offences.

Gaps

- Definitions of TFGBV remain uneven. Some statutes criminalise behaviours such as harassment but omit the gendered dimension or consent in intimate image sharing. **Example:** Malawi's Electronic Transaction and Cyber Security Act 2016[16] section 88 requires proof of intent to instil "reasonable fear for safety", which does not capture the humiliation of sexual exploitation inherent in image-based sexual abuse.
- Extra-territorial reach is limited in many jurisdictions, which complicates platform-hosted harms across national borders. **Example: Botswana's core cyber law**[17] predates the current platform ecosystem and does not fully address image-based sexual exploitation, although reform is underway through a GBV Bill.
- Laws recently enacted in the last five years may not appropriately deal with Artificial Intelligence (AI) related offences, which have a GBV perspective. For instance, creating unauthorised AI videos using a person's image.

Recommendations

- National Parliaments and Law Reform Commissions should adopt a harmonised definition of TFGBV that explicitly covers online forms of TFGBV such as harassment, stalking, sexual coercion and extortion, non-consensual production and dissemination of intimate images, grooming, and coerced content production, using the SADC Model Law as a legislative guide.
- At the same time, legal and policy reforms should be future-proofed, taking into account the fast-changing nature of digital technology, including the rapid expansion of Artificial Intelligence.
- Ministries of Justice and Attorneys-General should introduce clauses extending extra-territorial jurisdiction and establishing facilitator liability where online harms or trafficking activities are hosted or routed offshore.
- The SADC Parliamentary Forum (SADC-PF), in collaboration with national law reform institutions, should develop a Regional Model Definition Toolkit to support alignment and harmonisation of the definition of TFGBV across member states.
- Ministries of ICT and Data-Protection Authorities should update legacy cybercrime statutes and data-protection frameworks to include consent-based tests for intimate-image offences, deepfakes, and digital impersonation.

4.1.2 Human rights-based approach and policy direction

Why this matters
Rights to dignity, privacy, equality, and access to information should inform national GBV strategies that explicitly cover digital rights, safety, freedoms, and non-discrimination.

Progress (What is working)

- **South Africa:** The National Strategic Plan on Gender Based Violence and Femicide (2020–2030) references online harms in justice and safety pillars.[18]
- **Mozambique:** The National GBV Strategy integrates survivor support and coordination, which can be extended to TFGBV.[19]

Gaps

- Many national policies do not mention TFGBV. Migrant and child survivors face additional barriers.
- Government-allocated budget lines for digital safety, privacy support and platform engagement are rare.[20] The few that do include Mauritius, where the government funds the Computer Emergency Response Team (CERT-MU) for safety and privacy, which also engages platforms to mitigate cyber threats. Another example is in South Africa, where the government, in collaboration with partners like UNICEF, has funded child online safety programs and supports active engagement with digital platforms regarding platform abuse.[21]

Recommendations

- Ministries of Gender and National Gender Machineries should review and ensure that national GBV policies integrate digital safety components, survivor privacy standards, and access to online reporting channels.
- Ministries of Finance and Planning should allocate dedicated budget lines for TFGBV prevention and response within national GBV strategies and annual budgets.
- SADC-PF and the SADC Gender Unit should issue regional guidance on integrating TFGBV into gender justice frameworks, ensuring alignment with the SADC Protocol on Gender and Development, the Maputo Protocol, the AU Convention on Ending Violence against Women and Girls, and CEDAW commitments and obligations.
- Civil Society Organisations (CSOs) and Women's Rights Networks should advocate for inclusive digital policies that protect women and girls and marginalised groups and those impacted by intersectional forms of discrimination, including migrants, LGBTQ+ individuals, and rural women.

4.1.3 Access to justice and procedural protections

Why this matters
Survivors need rapid protective orders, admissible electronic evidence, and predictable disclosure pathways from service providers.

Progress (What is working)

- **Namibia:** The Electronic Transactions Act 2019[22] recognises the admissibility and integrity of data messages, used in court to accept chat records.
- **Botswana:** The Cybercrime Act 2018[23] provides preservation and production powers that investigators apply in TFGBV cases.
- **Mini case:** In **South Africa**, in terms of the Protection from Harassment Act 2011[24] courts are empowered to grant harassment orders to issue disclosure directions to unmask anonymous online abusers, and then issue extended orders to ban electronic contact.

Gaps

- Courts often lack standard forms for 24–72 hour data preservation, production orders and takedown directions.
- Chain-of-custody protocols for digital evidence are inconsistent, which risks exclusion at trial.

Recommendations

- Judicial Training Institutes and Prosecutor-General's Offices should develop and roll out training modules on digital evidence collection, chain of custody, and survivor-centred questioning.
- Chief Justices and Judicial Councils should issue practice directions on standard forms for electronic evidence preservation, production orders, and content takedown, with 24–72-hour response timelines.
- Ministries of Justice should designate single points of contact (SPOCs) within prosecution and police cyber units to handle TFGBV cases and coordinate with online platforms.
- Law Societies and Bar Associations should support pro bono representation for digital rights for TFGBV survivors.

4.1.4 Prohibition of gender-based violence and attendant procedures

Why this matters
Criminal offences and sentencing factors must reflect modern online harms and the exploitation cycle used in trafficking.

Progress (What is working)

- **South Africa:** Cybercrimes Act 2020 section 16[25] used in prosecutions such as **KS v AM & AHM[26]** for the creation and dissemination of image-based sexual abuse and defaming the victim.
- **Zimbabwe:** The Cyber and Data Protection Act creates an offence for the "transmission of intimate images without consent" in Section 164E.[27]
- **Mozambique:** Law 6/2008 on Human Trafficking defines "Pornography" broadly, including through the use of ICT.[28]

Gaps

- Many states still lack explicit offences for non-consensual sharing of intimate images, sexual coercion and extortion, livestreamed abuse and online grooming.
- Trafficking statutes do not always name ICTs as means of recruitment, coercion or control.

Recommendations

- **National Parliaments** should enact explicit offences for non-consensual sharing of intimate images, sexual coercion and extortion, livestreamed abuse, online grooming, and the creation or circulation of child sexual abuse material.
- **Ministries of Justice and Anti-Trafficking Committees** should amend trafficking laws to recognise **online recruitment, coercion, and digital control** as elements of exploitation.
- **Prosecution Services and Police Cyber Units** should issue **charging and investigation guidelines** linking TFGBV and trafficking offences, with survivor-protection measures.
- **Regional Judicial Training Networks** under **SADC-PF** should host annual exchanges on case law, sentencing, and TFGBV jurisprudence.

4.1.5 Early and effective response mechanisms and referral systems

Why this matters
First contact and referral determine safety, evidence preservation and survivor trust, especially when threats persist online.

Progress (What is working)

- **Eswatini:** Cybercrime Act 2022[29] details preservation and disclosure procedures that support rapid investigations.
- **Zambia:** Cyber Security and Cyber Crimes Act 2021[30] enables coordinated response and data requests through a national CERT.

Gaps

- Few countries operate 24/7 contact points or joint TFGBV protocols between police, regulators and shelters.
- School and campus pathways for grooming, sexual coercion, and extortion reporting are underdeveloped.

Recommendations

- Ministries of Home Affairs and Police Services to establish national TFGBV Response Units with a 24/7 hotline, digital-forensics support, and an on-call prosecutor.
- Inter-Agency GBV Committees to adopt Standard Operating Procedures (SOPs) that integrate digital safety planning, evidence preservation, and referral to psychosocial and legal services.
- Ministries of Education should develop and enforce school and university reporting mechanisms for online grooming, sexual coercion, and extortion, linked to safeguarding protocols.
- SADC-PF to ensure parliamentary initiatives in relation to coordinated cross-border rapid-response protocols for digital trafficking investigations and facilitate mutual legal assistance among Member States.

4.1.6 Prevention, protection, support and intervention measures

Why this matters
Survivor-centred services must include digital safety, privacy support and practical help to remove harmful content.

Progress (What is working)

- **Lesotho[31], Botswana[32], Zimbabwe[33]:** Domestic-violence laws allow protection orders that restrain electronic contact, which shelters and legal-aid groups use in practice.
- Emerging practice of court-ordered disclosure against platforms to identify perpetrators.

Gaps

- Shelters rarely offer digital safety planning, device security checks, or content takedown assistance.
- Privacy and anonymity safeguards in proceedings are uneven, especially for child and migrant survivors.

Recommendations

- Ministries of Social Welfare, Gender, and ICT should fund digital safety services within shelters and one-stop centres, including account security support, evidence preservation, and platform takedown assistance.
- Data Protection Authorities and Communications Regulators should establish survivor-led takedown mechanisms and publish guidance for online platforms on privacy and survivor protection.
- Courts and Ministries of Justice should guarantee anonymity and closed-court options for TFGBV and online trafficking survivors.
- CSOs and Survivor Networks should implement community-based digital literacy programmes to empower women and girls to navigate online spaces safely

4.1.7 Data, capacity, public awareness, monitoring and evaluation

Why this matters
Decision-makers need reliable signals about TFGBV incidence, justice outcomes and service performance to steer reform.

Progress (What is working)

- **Mauritius, Botswana, Seychelles, South Africa:** Data-protection authorities are operational and can receive privacy complaints linked to TFGBV.
- Some police services publish cybercrime statistics that can be disaggregated.

Gaps

- TFGBV indicators are rarely integrated into GBV information systems.
- Capacity for gender-sensitive digital investigations is limited across police and prosecution services.

Recommendations

- National Statistical Offices and GBV Coordination Units to integrate TFGBV indicators into GBV information systems and produce annual administrative reports on online violence.
- Police, Prosecutor, and Judicial Academies to incorporate TFGBV modules in basic and continuous training curricula.
- The SADC Gender Unit coordinates regional data harmonisation and develops minimum indicators for TFGBV monitoring across member states.
- Media Councils and Communications Ministries should run public-awareness campaigns on online grooming, sexual coercion and extortion, and digital safety in multiple languages and accessible formats.

4.1.8 Enforcement, compliance and regulatory mechanisms

Why this matters
Regulatory powers can operationalise platform cooperation, transparency, and compliance, which are essential for timely takedown and evidence access.

Progress (What is working)

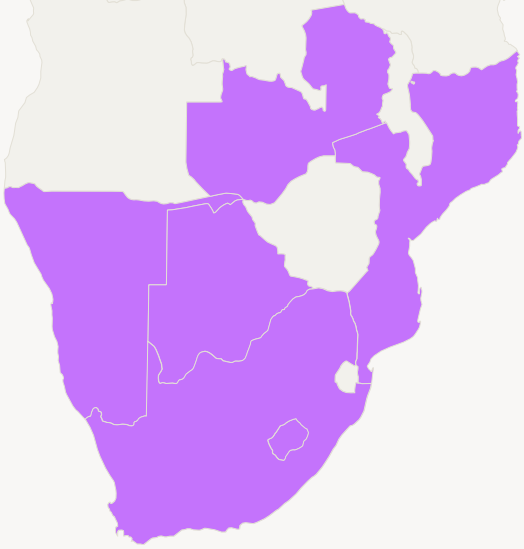
- **Botswana:** The Data Protection Act 2024 establishes a commission with the authority to address privacy harms that often sit behind TFGBV.
- **South Africa and Mauritius:** Regulators have issued public notices and guidance on privacy and online harms. In Mauritius, the Data Protection Act 2017 actively protects data subjects in relation to their personal data and requires the mandatory registration of data controllers and data processors, thereby amplifying the protection against TFGBV, which often relies on the use of unprotected data.

Gaps

- Most states lack clear notice-and-action rules, trusted-flagger arrangements and time-bound takedown standards.
- Budgets for enforcement and cross-border cooperation are thin.

Recommendations

- Data Protection and Communications Regulators should issue platform cooperation regulations requiring notice-and-action procedures, standard response timelines, and privacy safeguards.
- Ministries of ICT should sign Memoranda of Understanding (MoUs) with major online platforms to establish trusted-flagger channels for TFGBV and trafficking content.
- National Treasuries and Gender Ministries should earmark GBV-fund allocations for TFGBV enforcement and cross-border coordination.
- SADC-PF and SADC Secretariat should create a Regional TFGBV Implementation Tracker to monitor progress on domestication and enforcement of the Model Law.



5. Illustrative case studies

1. **South Africa – Criminalising NCII:**
   Section 16 of the Cybercrimes Act 2020 makes it an offence for a person to intentionally share an intimate image of another person via an electronic message service without their consent.[34]

2. **Mozambique – Tech-enabled Trafficking Recruitment:**
   Police dismantled a Facebook-based recruitment ring using Law No. 6/2008 on Human Trafficking. The case underscored how explicit mention of technology in law enables prosecution.

3. **Namibia – Admitting Digital Evidence:**
   In *S v Nestor [2023]*[35]*, the* court extended the admissibility of electronic documents without the need to authenticate as long as there is no other proof to the contrary. This illustrates a progression in the Law of Evidence toward the acceptance of electronic evidence.

4. **Lesotho – Recognising Technological Abuse:**
   The Counter Domestic Violence Act (2022)[36] defines technological abuse, allowing courts to restrain electronic contact.

5. **Botswana – Pending GBV Bill (2025)[37]:**
   A forthcoming Bill aims to integrate cyber-harassment and image-based abuse into GBV legislation, showing reform momentum.

6. **Zambia – Cyber Security and Cyber Crimes Act (2021):**
   Created a Cyber Security Advisory Council to coordinate digital-violence investigations, an example of institutional collaboration.

7. **Mauritius** – Cybersecurity and Cybercrme Act (2021)

Sections 17 and 18 of the Act prohibit cyberbullying and cyber extortion and specify that these offences carry heavy criminal penalties, including penal servitude for up to 20 years.[38]

6. Good practices in SADC

Country / Instrument	What Works	Safeguards / Lessons
South Africa – Cybercrimes Act 2020	Explicit NCII offence with successful prosecutions (*S v SB 2022*).	Pair legal reform with survivor privacy and digital-evidence support.
Mozambique – Law 6/2008 Art 15	Recognises internet promotion of trafficking.	Demonstrates how trafficking frameworks can include digital means.
Botswana – Data Protection Act 2024	Creates an independent regulator and privacy complaint process.	Establishes redress mechanisms for survivors of online harm.
Eswatini – Cybercrime Act 2022	Details electronic evidence preservation processes.	Serves as a regional model for procedure and training.
Lesotho – DV Act 2022	Defines technological abuse and mandates the issuance of immediate protection orders.	Practical tool for survivor protection in digital contexts.

7. Recommendations

Regional level – SADC-PF and Secretariat

- Develop a **Model TFGBV Amendment Protocol** to the SADC Model Law, which can also identify and address the legal implications of emerging trends such as the growth of AI and its influence on GBV.
- Establish a **TFGBV Observatory** under the SADC Gender Unit to track data and trends.
- Create **regional mutual-assistance templates** for digital evidence and content takedown.
- Facilitate **annual parliamentary sessions** on TFGBV and digital trafficking.

National level – Parliaments and Ministries of Justice

- Fast-track cybercrime, GBV, and data protection bills.
- Amend trafficking and GBV laws to explicitly address ICT-enabled offences.
- Introduce **electronic protection orders** within 48 hours.
- Develop **training curricula** for prosecutors and judges on TFGBV case management.

Regulators and law enforcement

- Establish **trusted-flagger agreements** with social media platforms.
- Designate **24/7 cybercrime focal points** to support survivors.
- Publish **annual reports** on TFGBV enforcement and takedown actions.

Civil society and service providers

- Expand shelter mandates to include **digital safety and online takedown support**.
- Provide legal and psychosocial services adapted to online harms.
- Lead **public awareness campaigns** on sexual coercion and extortion, grooming, and safe digital practices.

Conclusion

TFGBV is rapidly reshaping how harm is experienced, perpetrated, and perpetuated across the SADC region. While many member states have made important progress in strengthening gender-based violence and cybercrime laws, gaps remain where legal frameworks do not fully capture the realities of digital abuse, exploitation, and coercion. **As digital technologies become more embedded in everyday life, legal and policy responses must evolve to ensure that women and girls are protected both online and offline.**

The SADC Model Law on Gender-Based Violence provides a strong regional foundation for addressing GBV. However, effectively responding to technology-facilitated forms of violence requires updating and operationalising this framework to reflect the ways technology is used to perpetrate harm, facilitate exploitation and silence survivors. Strengthening legislation alone will not be sufficient. Survivor-centred justice systems, specialised institutional capacity, clear platform accountability mechanisms and regional cooperation on digital evidence and cross-border enforcement are all critical to closing the gap between law and lived reality.

By adopting the recommendations outlined in this report, SADC member states and regional institutions have an opportunity to build a more coherent and future-ready response to gender-based violence in the digital age. Doing so will help ensure that legal protections keep pace with technological change and that survivors are able to access effective remedies, protection, and support. A coordinated regional approach can position SADC as a leader in advancing rights-based, survivor-centred responses to TFGBV.

Annexure 1: 16-Country domestication snapshot

Country	TFGBV Offence	Data Protection	Trafficking Mentions ICTs	GBV Law Covers Electronic Abuse	Model Law Domesticated
South Africa	✓	✓	✓	✓	Partial
Namibia	✗	Bill	✗	✓	Partial
Botswana	✓	✓	✓	✓	Draft GBV Bill
Zimbabwe	✓	✓	✗	✓	Partial
Mozambique	✗	Bill	✓	✓	Partial
Angola	✗	✓	✗	✗	Pending
Eswatini	✓	✗	✗	✓	Partial
Lesotho	✓	Bill	✗	✓	Partial
Madagascar	✗	Bill	✓	✗	Partial
Malawi	✗	Bill	✗	✗	Partial
Mauritius	✗	✓	✓	✓	Partial
Seychelles	✗	✓	✗	✗	Partial
Tanzania	✗	✗	✓	✗	Draft GBV Bill
Zambia	✓	✓	✓	✓	Partial
DRC	✗	✓	✗	✗	Low
Comoros	✗	✗	✗	✗	Low

Endnotes

1 UN Women. (2025). Digital violence in East and Southern Africa: Urgent action needed to protect women and girls online. https://africa.unwomen.org/en/stories/press-release/2025/11/digital-violence-in-east-and-southern-africa-urgent-action-needed-to-protect-women-and-girls-online#:~:text=The%2016%20Days%20of%20Activism%20against%20Gender%2DBased%20Violence%20is,safe%20and%20inclusive%20for%20all.

2 AU (2025) African Union Convention on Ending Violence Against Women and Girls, Article 3.

3 SADC Model Law on Gender Based Violence. https://www.sadcpf.org/index.php/en/documents/model-laws/sadc-model-law-on-gender-based-violence-2/download.

4 NORC. (2022). A landscape analysis of technology-facilitated sexual violence in the Asia-Pacific region. https://www.norc.org/research/projects/technology-facilitated-sexual-violence.html.

5 AU (2025) African Union Convention on Ending Violence Against Women and Girls, Article 1(b).

6 MISA.(2024) A study of technology facilitated gender-based violence in Southern Africa.https://unesdoc.unesco.org/ark:/48223/pf0000390886.

7 World Bank Group. (2024). Digital Transformation Drives Development in Africa. https://www.worldbank.org/en/results/2024/01/18/digital-transformation-drives-development-in-afe-afw-africa#:~:text=The%20region's%20digital%20infrastructure%20coverage,according%20to%202023%20GSMA%20data.

8 GSMA. *Despite improvements, Sub-Saharan Africa has the widest usage and coverage gaps worldwide.* Blog, 28 October 2025. Available at: https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-for-development/blog/despite-improvements-sub-saharan-africa-has-the-widest-usage-and-coverage-gaps-worldwide/.

9 GSMA. *The Mobile Gender Gap Report 2025.* March 2025. Available at: https://www.gsma.com/r/gender-gapthe justice, Information and Communication Technology (ICT), education, and social welfare/.

10 Counter Domestic Violence Act (2022). (Lesotho) .https://lesotho.unfpa.org/sites/default/files/pub-pdf/act_no._14_of_2022_counter_domestic_violence_act.pdf.

11 WOSSO. (2025). GBV in SADC: Progress, challenges, and pushing forward. https://wosso.org/resources_and_news/gbv-in-sadc-progress-challenges-and-pushing-forward.

12 Cybercrimes Act, 2020. (South Africa). https://www.gov.za/documents/acts/cybercrimes-act-19-2020-english-afrikaans-01-jun-2021.

13 Counter Domestic Violence Act, 2022. (Lesotho). https://lesotho.unfpa.org/en/publications/counter-domestic-violence-act.

14 Cyber and Data Protection Act, 2021. (Zimbabwe). https://www.veritaszim.net/node/5522.

15 Cybersecurity and Cybercrime Act, 2021 (Mauritius), Part III.

16 Electronic Transaction and Cyber Security Act 2016. (Malawi). https://malawilii.org/akn/mw/act/2016/33/eng@2017-12-31.

17 Cybercrime And Computer Related Crimes Act, 2018. (Botswana). https://www.bocra.org.bw/sites/default/files/documents/18%20Act%2029-06-2018%20Cybercrime%20and%20Computer%20Related%20Crimes.pdf.

18 The National Strategic Plan on Gender Based Violence and Femicide (2020–2030). (South Africa). https://www.gov.za/sites/default/files/gcis_document/202006/stratplan-gbvs.pdf.

19 World Vision. (2025). Improving Access and Strengthening Support for Gender-Based Violence Survivors. https://www.wvi.org/stories/mozambique/improving-access-and-strengthening-support-gender-based-violence-survivors#:~:text=A%20new%20Integrated%20Support%20Centre%20(CAI)%20in,centralizes%20essential%20services%20for%20gender%2Dbased%20violence%20survivors.

20 South African Institute of International Affairs (SAIIA). (2024). Futures of Digital Rights in SADC: Towards a Common Approach to Digital Protection and Data Justice. https://saiia.org.za/research/futures-of-digital-rights-in-sadc-towards-a-common-approach-to-digital-protection-and-data-justice/#:~:text=Summary,shaped%20the%20digital%20rights%20discourse.

21 UNICEF South Africa. Strengthening Children's Online Safety in South Africa. https://safeonline.global/unicef-south-africa/#:~:text=Through%20new%20funding%20by%20Safe,guide%20to%20drive%20national%20action.

22 The Electronic Transactions Act, 2019. (Namibia). https://namiblii.org/akn/na/act/gn/2020/75/eng@2020-03-16.

23 Cybercrime And Computer Related Crimes Act, 2018. (Botswana). https://www.bocra.org.bw/sites/default/files/documents/18%20Act%2029-06-2018%20Cybercrime%20and%20Computer%20Related%20Crimes.pdf.

24 Protection from Harassment Act, 2011. (South Africa). https://www.gov.za/documents/acts/protection-harassment-act-17-2011-05-dec-2011.

25 Cybercrimes Act, 2020. (South Africa). https://www.gov.za/documents/acts/cybercrimes-act-19-2020-english-afrikaans-01-jun-2021.

26 KS v AM & AHM [2024] 21-28121 (GJ). https://itlawco.com/ks-v-am-ahm-a-case-of-revenge-porn-and-defamation/.

27 Cyber and Data Protection Act [Chapter 12:07]. https://www.veritaszim.net/sites/veritas_d/files/Cyber%20%26%20Data%20Protection%20Act%20Cap1207%20No%205%20of%202021%20gaz%202022-03-11.pdf.

28 ECPAT. (2020). Sexual Exploitation of Children in Mozambique Submission for the Universal Periodic Review of the Human Rights situation in Mozambique. https://upr-info.org/sites/default/files/documents/2021-07/js3_upr38_moz_e_main.pdf.

29 Computer Crime and Cybercrime Act, 2022. (Eswatini). https://www.esccom.org.sz/legislation/COMPUTER%20CRIME%20&%20CYBERCRIME%20ACT.pdf.

30 Cyber Security and Cyber Crimes Act. (2021). Zambia. https://www.parliament.gov.zm/node/8832.

31 The Counter Domestic Violence Act, 2022. (Lesotho). https://www.webbernew.com/uploads/GG%20No.%2072%20of%202022.pdf.

32 Domestic Violence Act, 2008. (Botswana). https://policyvault.africa/policy/domestic-violence-act-2008/.

33 Domestic Violence Act [CHAPTER 5:16] (Zimbabwe). https://clr.africanchildforum.org/Legislation%20Per%20Country/Zimbabwe/zimbawe_domesticviolence_2007_en.pdf.

34 SD Law – Simon Dippenaar & Associates Inc. (2022). Cybercrimes Act 2020 and data messages. https://www.sdlaw.co.za/articles/cybercrimes-act-2020-data-messages/#:~:text=The%20Act%20was%20signed%20into,the%20outcome%20of%20criminal%20prosecution.

35 *S v Nestor* (CC 09/2022) [2023] NAHCMD 339. https://ejustice.jud.na/High%20Court/Judgments/Criminal/S%20v%20Nestor%20(CC%2009%202022)%20[2023]%20NAHCMD%20339%20(%2031%20May%202023).doc.

36 The Counter Domestic Violence Act, 2022. (Lesotho). https://www.webbernew.com/uploads/GG%20No.%2072%20of%202022.pdf.

37 NewEra Live. (2025). https://neweralive.na/chombo-calls-for-inclusion-of-women-in-leadership/.

38 Cybersecurity and Cybercrime Act (2021), sections 17 and 18 available at https://www.icta.mu/documents/2021/12/cybersecurity_act_2021.pdf.

Equality Now

A just world for all women and girls

equalitynow.org

programs@equalitynow.org

@Equality Now Africa

SADC

Parliamentary Forum

Forum Parlementaire

Fórum Parlamentar

sadcpf.org

info@sadcpf.org

@SADC Parliamentary Forum