AFRICAN WOMEN'S DEVELOPMENT FUND

CRAWN TRUST
Community Advocacy and Awareness Trust

Gap Analysis Report on Technology-Facilitated Gender -Based Violence (TFGBV) in Kenya

Contents

ACKNOWLEDGEMENT

We extend our profound appreciation to The African Women's Development Fund (AWDF) for the invaluable partnership and support to the Community Advocacy and Awareness Trust (CRAWN Trust) in undertaking this Gap Analysis on Technology-Facilitated Gender-Based Violence (TFGBV) in Kenya. This support has significantly advanced efforts aimed at safeguarding the rights, agency, dignity, and voices of women and girls in Kenya.

We further convey our sincere gratitude to the diverse state and non-state actors who generously contributed their expertise, insights, and time to this undertaking. Their perspectives enriched the analysis and strengthened the quality and relevance of the report.

We pay special tribute to the survivors who courageously shared their lived experiences in the interest of advancing justice, accountability, and systemic reform. We are particularly grateful to Lorraine Ong'injo of the ReBuilding Community Organization and Waruguru Muriithi of the Wangu Kanja Foundation for mobilizing and convening survivors to participate in an experience-sharing session that greatly informed the Gap Analysis. We also extend our heartfelt appreciation to the Wangu Kanja Foundation for graciously hosting the session.

Finally, we acknowledge with deep appreciation the exemplary dedication and professionalism of the consultant, Mutheu Nyagah Khimulu of the Mutheu Khimulu Consultancy, whose technical expertise, diligence, and commitment were instrumental in conducting this analysis and producing this report.

STATEMENT OF PRINCIPLE:

RIGHTS-BASED, FEMINIST, AND CONSTITUTIONALLY GROUNDED APPROACH.

This gap analysis is undertaken in alignment with **the core values of CRAWN Trust[1],** including the advancement of women's rights, feminist legal analysis, access to justice, and the protection of democratic space, as well as **the mission of the African Women's Development Fund[2]** to support rights-based, women-led initiatives that challenge structural inequality and systemic violence. **It is grounded in the Constitution of Kenya (2010)[3]** and is informed by a commitment to gender equality, human dignity, and accountability in both physical and digital environments.

The gap analysis explicitly upholds the right to freedom of expression guaranteed under Article 33 of the 2010 Kenyan Constitution, recognizing its centrality to democratic participation, feminist organizing, and civic engagement. At the same time, it affirms that constitutional protection does not extend to conduct that propagates violence, incites harm, or exploits digital spaces to intimidate, harass, or silence women and girls. Consistent with Article 28, which guarantees the inherent dignity of every person, and Article 27, which affirms equality and freedom from discrimination, this gap analysis recognises Technology-Facilitated Gender-Based Violence (TFGBV) as a direct threat to women's dignity, safety, and equal participation in public life.

In line with Article 48, which guarantees access to justice, and Article 21, which places an obligation on the State to respect, protect, promote, and fulfil rights and fundamental freedoms, this gap analysis seeks to strengthen legal and institutional responses to technology-facilitated gender-based violence through evidence-based, survivor-centred, and gender-responsive recommendations. It does not seek to gag, chill, or constrain lawful expression, legitimate dissent, or civic participation. Rather, it is premised on a clear and principled distinction between constitutionally protected speech and conduct that causes real and demonstrable harm, including abuse, harassment, intimidation, and other forms of digital violence disproportionately affecting women and girls across all demographics.

Any recommendations emerging from this gap analysis will be guided by the principles of proportionality, necessity, and legality, ensuring that proposed enforcement and policy measures are rights-respecting and narrowly tailored to prevent harm and secure accountability without enabling censorship or misuse. This framing reflects CRAWN Trust's feminist commitment to transformative justice, the African Women's Development Fund's emphasis on systemic change and women's agency, and Kenya's constitutional promise of dignity, equality, and justice for all.

Daisy Amdany

Executive Director,

CRAWN Trust

[1] *https://crawntrust.org/about/*
[2] *https://awdf.org/who-we-are/vision-mission/*
[3] *https://www.parliament.go.ke/sites/default/files/2017-05/The_Constitution_of_Kenya_2010.pdf*

EXECUTIVE SUMMARY

This gap analysis forms part of the "Safe Spaces, Strong Voices" project implemented by the Community Advocacy and Awareness Trust (CRAWN Trust) with funding support from the African Women's Development Fund (AWDF). It presents a rigorous, feminist, and survivor-centered diagnostic of Kenya's legal, institutional, and policy response to Technology Facilitated Gender Based Violence against women and girls.

The analysis draws on a comprehensive desk review, a multi-sectoral virtual stakeholder consultation convened in February 2026, Key Informant Questionnaire responses from state actors, constitutional office holders, civil society organisations, feminist groups and frontline practitioners, and the direct testimony of survivors collected through a confidential questionnaire administered at the Wangu Kanja Foundation in March 2026.
The assessment is grounded in the Constitution of Kenya 2010, Kenya's domestic legislative framework, and the full spectrum of binding and persuasive regional and international human rights standards applicable to digital gender-based violence.

Kenya occupies a paradoxical position in the global digital landscape. As the birthplace of Mpesa, which is ranked amongst the top ten most influential projects in human history, and Ushahidi, a platform that reshaped global democratic activism, the country has emerged as one of the world's fastest growing digital economies.

Kenya's mobile penetration stands at 149.4%, and has a mobile money penetration at 91%. Yet the same technological ecosystem has created an expanded attack surface within which women and girls bear a disproportionate and escalating burden of harm.

Approximately 95% of aggressive online behaviour and denigrating digital imagery disproportionately targets women. Up to 60% of women leaders, journalists, activists and students have reduced or abandoned digital participation to protect themselves from sustained harassment, threats and reputational attacks. This phenomenon, described as radio silencing, represents a structural threat not only to individual wellbeing but also to Kenya's democratic participation, leadership pipeline and knowledge economy.

In 2024 Kenya recorded 579 femicide cases, many preceded by digital threats and stalking, placing the lethal continuum between technology-facilitated violence and physical harm beyond reasonable dispute.

The gap analysis identifies nine interconnected categories of systemic failure in Kenya's current TFGBV response architecture.

The first is the definitional and legislative gap. Kenya lacks a standalone gender responsive TFGBV legal framework, a statutory definition of TFGBV as a distinct category of harm, and legal provisions addressing AI generated deepfakes, voice cloning, synthetic intimate imagery, cryptocurrency enabled sextortion and other evolving forms of TFGBV. **This gap is compounded by the constitutional suspension in October 2025 of key cyber harassment provisions under the Computer Misuse and Cybercrimes Act (CMCA), following the High Court finding in Reuben Kigame Lichete & Kenya Human Rights Commission (KHRC) vs. The Attorney General & Others (HCCRPET/E673/2025)**[4], that enhanced penalties were overbroad and insufficiently precise. The result is an enforcement vacuum that benefits perpetrators and leaves survivors without the statutory protection that the recent amendments were intended to provide.

The second category is the enforcement and evidentiary deficit. The DCI National Digital Forensic Laboratory lacks adequate tools and personnel, investigators lack training and protocols to collect and preserve digital evidence to prosecution standards, and backlogs mean that survivors' devices are frequently held for more than a year, compounding trauma and economic precarity.

The third category is institutional fragmentation. Survivors of AI generated intimate image abuse may be required to navigate multiple institutions simultaneously including the DCI, the Office of the Data Protection Commissioner, Policare, the Office of the Director of Public Prosecutions and the Judiciary, without an integrated referral pathway, case management system or single point of contact.

The fourth category is the survivor centred remedy gap. Kenya currently has no emergency content removal orders, no right to be forgotten, no interim injunctive relief and no statutory compensation framework for the reputational, psychological, economic and professional harm caused by TFGBV. Even successful prosecutions therefore fail to address the ongoing injury caused by harmful content that remains publicly accessible.

The fifth category is the emerging technology governance void. AI generated deepfakes, nudify applications, voice cloning and algorithmically amplified misogynistic content fall outside the scope of current legislation, and the National AI Strategy 2025 to 2030 does not address the gendered dimensions of AI risk.

The sixth category is the socio cultural and awareness gap. 78% of survivors who participated in the study's questionnaire did not know where to report or seek help at the time of the incident, underscoring the structural failure of public awareness alongside legal and institutional shortcomings.Three additional dimensions extend the conventional understanding of TFGBV.

The seventh category is that children and minors represent a critical and currently under protected population. The rollout of the Competency Based Curriculum (CBC) has introduced AI driven educational tools into classrooms without parental awareness of

[4] *https://khrc.or.ke/wp-content/uploads/2025/10/9732195C-0CA5-4391-9F17-A66340A6A497.pdf*

data collection practices, while child specific provisions are absent from the Artificial Intelligence Bill 2026. All this whilst in many instances TFGBV against girls begins in school environments.

The eighth category pertains to specific demographic groups including women with disabilities, elderly women and rural women face intersecting vulnerabilities that a one size fits all legal framework cannot address.

And finally, the ninth category entails the supply side of TFGBV, including the transnational manosphere ecosystem and platform monetisation models that algorithmically amplify harassment, requires regulatory responses that address not only harm, but also the commercial incentives and ecosystems that sustain it.

Additionally, the gap analysis examines fifteen domestic legal instruments all emanating from the mother of all laws, the Kenya Constitution 2010, in addition to fourteen regional and international frameworks including the Maputo Protocol, the AU Convention on Ending Violence Against Women & Girls, the Budapest & Malabo Conventions and the ILO Convention 190. The analysis identifies specific gaps, required amendments and the justification for each. It also provides a detailed assessment of the Artificial Intelligence Bill 2026 currently before the Senate, concluding that while it represents a meaningful starting point for Kenya's AI governance, it should not be passed as it currently reads, as it requires significant amendment to prevent further institutional fragmentation, deliver gender responsive regulation and protect Kenyan children from harms already occurring on their devices and in classrooms.

Looking ahead, the analysis also addresses the quantum computing threat to digital evidence integrity and the harvest now decrypt later risk to survivor confidentiality, arguing that all digital forensic and evidence preservation investments must be built with post quantum cryptographic resilience as a baseline requirement from inception.

The recommendations emerging from this analysis are organised across nine thematic areas. These include enacting a standalone TFGBV Act informed by the UN Women Model Framework for Legislation on Technology Facilitated Violence Against Women and Girls, urgently redrafting the suspended CMCA provisions in constitutionally compliant terms, and amending the Data Protection Act, Sexual Offences Act, Protection Against Domestic Violence Act, Kenya Information and Communications Act, Employment Act, Children Act, National Cohesion and Integration Act and the National Gender and Equality Commission Act to address TFGBV dimensions.

The gap analysis calls for the establishment of a gazetted national TFGBV coordination framework, investment in digital forensic capacity with post quantum resilience as a design requirement, creation of specialist prosecution capacity within the Office of the Director of Public Prosecutions, strengthening of county level gender response, and enforceable platform accountability obligations including Urgent Digital Protection Orders with twenty-four-hour compliance timelines.

The gap analysis further recommends the creation of a comprehensive survivor support infrastructure that removes financial barriers and integrates psychosocial, legal and economic empowerment services, investment in disaggregated data and a national TFGBV data observatory, full operationalisation of Kenya's accession to the Budapest and Malabo Conventions and ratification of ILO Convention 190, and commissioning of a macroeconomic impact assessment to integrate digital safety into Kenya's public expenditure framework as a development investment.

Addressing TFGBV is not a gender equality initiative in competition with Kenya's economic development priorities. It is a precondition for those priorities to be realised. Every woman driven from digital space by harassment represents a lost voice, a lost vote, a lost professional contribution, and a lost democratic perspective that Kenya's knowledge economy cannot afford. Whilst this analysis centers women and girls as the population most severely, most frequently, and most systematically targeted by technology-facilitated gender-based violence, it does so in full recognition that TFGBV also harms boys and men, but whose reporting rates remain significantly lower due to stigma, inadequate awareness of available mechanisms, and the absence of legal frameworks that explicitly acknowledge their vulnerability.

To this end, every legislative and institutional reform recommended in this gap analysis is designed with gender-neutral protective provisions, recognizing that strengthening Kenya's digital safety architecture benefits all persons who experience digital harm. The findings of this gap analysis were presented during a stakeholder validation virtual meeting held on 22 April 2026, where participants provided feedback, responses, and additional contributions that have been incorporated into this work. At the conclusion of the session, stakeholders were formally asked whether they validated the gap analysis, and the validation was unanimous. A Kenya in which technology-facilitated violence is effectively named, prosecuted, remedied, and prevented is a Kenya that is safer, more democratic, more economically productive, and more just for all its citizens, regardless of gender.

MUTHEU NYAGAH KHIMULU

LLM. Cyber Security, Counter Terrorism & Crisis Management,

Lead Consultant, Gap Analysis on TFGBV in Kenya April 2026.

https://www.linkedin.com/in/mutheu-khimulu-law/

CHAPTER 1.
BACKGROUND AND RATIONALE FOR A STRATEGIC INTERVENTION.

1.1 THE DIGITAL FRONTIER: A Paradox Of Progress And Peril.

1.1.1 From the Cradle of Humankind to the Cradle of Innovation:

Kenya holds a dual heritage of global distinction. It is recognized as the Cradle of Humankind, **with the most diverse record of human evolutionary history stretching from the seven-million-year-old Orrorin Tugenensis to the Turkana Boy[5],** and it has ascended as the Cradle of Innovation through the development of homegrown technologies, that have reshaped global industries. This dual identity is not incidental to a gap analysis on technology-facilitated gender-based violence. It is essential context because, the same innovative genius that produced Kenya's most celebrated technological exports, has created a digital landscape whose benefits are being systematically denied to the women and girls, who constitute half of its population.

1.1.2 The Pillars of Kenyan Innovation:

Kenya's ascent as a technology powerhouse is anchored by two revolutionary exports. **Ushahidi[6]** a Kenyan-made crowdsourcing engine, redefined digital activism and disaster response globally. It was deployed by the 2012 Obama Presidential Campaign to map voter suppression in real time and utilized by the United States Marine Corps and Coast Guard to direct life-saving aid during the Haiti earthquake. **M-Pesa[7]** achieved world-leading market penetration by successfully banking the unbanked,and was ranked by the Project Management Institute as the ninth most influential project in human history, surpassing the launch of the International Space Station and the founding of Netflix.

1.1.3 The Double-Edged Sword of the Silicon Savannah:

As of early 2026, Kenya's digital ecosystem has reached a historic zenith, with mobile penetration standing at 149.4%, SIM registrations climbing past 78 million, and mobile money penetration holding steady at 91% (CA First Quarter Sector Statistics 2025/2026). However, this transformation represents a profound paradox. While these metrics signal unprecedented platforms for economic agency and voice, they simultaneously delineate a vast and expanded attack surface for Technology-Facilitated Gender-Based Violence (TFGBV). The very tools that have propelled Kenya to become one of the world's fastest-growing digital economies are being weaponized with precision, and the same digital transformation that offers revolutionary empowerment, is also being exploited to target and silence, turning celebrated democratic and financial advances into sophisticated frontiers for digital harm.

1.1.4 The Democratic and Economic Cost of Digital Silencing:

Beyond individual harm, TFGBV is producing measurable macro-level consequences for Kenya's democratic participation, leadership pipeline, and knowledge economy. Evidence indicates that up to 60% of women in public and professional life reduce or abandon online participation as a protective response to sustained harassment, threats, and reputational attacks. This digital withdrawal also referred to as the radio silencing effect produces consequences that extend far beyond the individual survivor and has four dimensions i.e.:

- Erosion of democratic discourse and diversity of political participation.
- Reduced participation of women leaders, journalists, activists, and human rights defenders.
- Loss of talent and expertise in Kenya's knowledge and innovation economy.
- Constrained educational participation and professional visibility for young women and students.

[5] *https://artsandculture.google.com/story/how-kenya-became-the-cradle-of-humankind-national-museums-of-kenya/nQVBf9Oq7jWqIA?hl=en*
[6] *https://www.ushahidi.com/*
[7] *https://www.safaricom.co.ke/main-mpesa/m-pesa-services*

These violations are compounded by the weaponization of emerging technologies including AI-generated deepfakes and non-consensual intimate **imagery (NCII). A widely publicized case involving a Russian national who allegedly recorded and leaked intimate content**[8] of numerous Kenyan women without their consent, underscores how digitally-mediated violations can produce irreversible trauma, profound reputational ruin, and devastating personal loss. Kenyan law enforcement and cybercrime authorities have launched a formal i**nvestigation into the activities of this individual to address the cross-border dimensions of the violations**[11]**.**

Additionally, the domestic market is experiencing a proliferation of eyeglasses capable of recording, which are indistinguishable to the untrained eye. This significant technological advancement amplifies the likelihood of unconsented recording of Kenyans' activities, intimate or otherwise. These recordings can subsequently be weaponized to perpetuate technology-facilitated gender-based violence (TFGBV) and other cybercrimes, thus exploiting the stealthy nature of these devices to violate privacy on a broader scale. TFGBV must therefore be framed not only as a safety and human rights issue, but as a national development and economic inclusion challenge.

1.2 ARCHITECTURES OF ABUSE: Defining The Digital Continuum Of Violence.

1.2.1 The Systemic Nature of Technology-Facilitated Gender-Based Violence (TFGBV):

TFGBV is any act of gender-based violence that is committed, assisted, aggravated, or amplified through the use of digital technologies, online platforms, or information and communication technologies. TFGBV disproportionately targets women and girls and is rooted in structural gender inequality, power imbalances, and discriminatory social norms that are reproduced and intensified in digital environments.

The Association for Progressive Communications conceptualizes TFGBV as a pattern **of psychological, emotional, sexual, economic, and reputational harm carried out through digital means, defined not merely by the technology used but by the gendered intent, impact, and power relations underlying the abuse**[12]**.**

The UN Special Rapporteur on Violence Against Women[13] and **UNESCO**[14] have further recognized that digital technologies introduce distinct characteristics to gender-based violence, including scale, permanence, anonymity, transnational reach, and algorithmic amplification, each of which exacerbates harm and impedes access to justice.

At the regional level, the **African Commission on Human and Peoples' Rights, through Resolution 522 on the Protection of Women Against Digital Violence in Africa**[15], explicitly recognizes digital and online violence as a human rights violation and affirms state obligations to prevent, investigate, punish, and provide remedies for such violence.

1.2.2 The Artificial Intelligence Frontier: Algorithmic Aggression and Regulatory Voids:

Contemporary understandings of TFGBV now extends to emerging and AI-enabled harms including AI-generated deepfake sexual images, nudify and synthetic image applications, voice cloning, gendered disinformation, and automated harassment. In 2025, the European **Parliamentary Research Service confirmed that 98% of all deepfake content online constitutes non-consensual sexual imagery**[16]**,** of which 99% targets women and girls.

These forms of abuse expose significant gaps across four dimensions: attribution, given the difficulty of identifying perpetrators behind automated or synthetic content; evidence preservation, given the challenge of freezing volatile digital evidence before it is deleted or altered; jurisdiction, given the borderless nature of AI platforms that operate outside Kenyan territory; and survivor remedies, given the absence of specific rapid takedown mechanisms or rights to be forgotten for AI-generated harms.

1.2.3 From Legal Frameworks to Lived Reality:

A critical gap persists between law as written and law as experienced. The lived experiences of survivors and frontline practitioners provide a clear consensus that low reporting rates, procedural barriers, delays in digital evidence preservation, and limited awareness of available legal remedies and reporting channels, continue to compromise the effectiveness of existing frameworks. Bridging this gap requires integrating lived experiences, survivor testimony, and practitioner expertise into legal and policy reform, which is the methodological commitment that underpins this gap analysis.

[11] *https://www.youtube.com/watch?v=eX8QpeIQ6Z8*
[12] *https://www.apc.org/en/ending-technology-related-violence-against-women*
[13] *https://www.ohchr.org/en/special-procedures/sr-violence-against-women*
[14] *https://www.unesco.org/en/articles/online-violence-against-women-journalists*
[15] *https://achpr.au.int/en/adopted-resolutions/522-resolution-protection-women-against-digital-violence-africa-achpr*
[16] *https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf*

1.3 THE GENDERED GEOGRAPHY OF RISK: MAPPING THE "RADIO SILENCING" OF KENYAN WOMEN.

1.3.1 Three Critical Demographics:

The weaponization of digital innovation has produced a paradoxical landscape in which the tools of the Silicon Savannah have been repurposed into instruments of exclusion across three critical demographic groups.

Demographic	Key Finding	Source
Academic Frontline: Tertiary Institutions	64.4% of female students in Nairobi's higher learning institutions have personally experienced online violence, nearly double the rate of male peers at 35.5%. Nearly 90% of young adults have witnessed TFGBV.	UNFPA and Centre for Child and Gender Development, 2024 https://kenya.unfpa.org/en/news/new-study-reveals-extent-technology-facilitated-gender-based-violence-kenyas-higher-learning
Political and Media Vanguard: Women in Public Life	80% of women parliamentarians in Africa have faced psychological violence online. 75% of women media workers report digital abuse while performing their duties, contributing to a 63% increase in self-censorship.	Inter-Parliamentary Union survey https://www.ipu.org/resources/publications/issue-briefs/2021-11/sexism-harassment-and-violence-against-women-in-parliaments-in-africa ; UNESCO 2025 global report https://www.unesco.org/en/articles/new-report-unesco-warns-serious-decline-freedom-expression-and-safety-journalists-worldwide
Rural and Economically Vulnerable Women	Rural women face unique vulnerabilities including economic tech-abuse. 31.1% of women in regional audits report technology-enabled economic abuse by partners, including control over phone access and Mpesa credentials.	Johns Hopkins Bloomberg School of Public Health, 2024 https://publichealth.jhu.edu/sites/default/files/2025-10/Agile-2.0-2024-Women-s-Data-County-Specific-Dissemination-Brief-BUNGOMA.pdf

1.3.2 The Lethal Continuum: From Digital Threats to Femicide[17]

TFGBV is frequently a precursor to physical harm. In 2024, Kenya recorded 579 femicide cases, many of which were preceded by digital threats and stalking. From the non-consensual sharing of intimate imagery, to the rapid rise of AI-driven deepfakes, digital harm is currently outpacing the state's legislative capacity. This gap analysis accordingly adopts a Future-Back approach that frames Kenya's legal response as one that must anticipate the trajectory of technological change, rather than merely react to the harms it has already produced.

1.3.3 The Knowledge Economy and Educational Impact:

TFGBV is increasingly undermining participation in Kenya's higher education and research ecosystem. Students, early-career professionals, and young innovators face reputational attacks, non-consensual image sharing, and coordinated harassment that directly compromise academic participation and online learning, professional networking and digital career development, and the retention of women in STEM, digital entrepreneurship, and public leadership pathways. This creates a long-term pipeline risk for Kenya's digital economy and innovation leadership because, the radio silencing of women results in a homogenized knowledge base that lacks the diverse insights necessary to build inclusive technology solutions, ultimately leaving Kenyan products less competitive in a global market that demands gender-responsive innovation.

17https://www.unesco.org/en/articles/call-action-confronting-alarming-rise-gender-based-violence-and-femicide-kenya

1.4 AFRICAN WOMEN'S VOICES IN THE DIGITAL AGE: FROM SYSTEMIC SILENCE TO DIGITAL POWER.

1.4.1 The Spectrum of Digital Harm in Kenya:

The legal and technical framework of this gap analysis addresses a wide spectrum of TFGBV, spanning established cybercrimes and emerging AI-driven threats, including those outlined in the chart below.

Form of TFGBV	Description	Current Legal Status
Cyberstalking and Surveillance	GPS tracking, stalker ware, or persistent digital monitoring of a partner's movements, communications, and activities.	Section 27 of the Computer Misuse and Cybercrimes Act (CMCA) criminalises cyber-harassment; however sophisticated surveillance provisions remain a legal grey area. CMCA link: https://new.kenyalaw.org/akn/ke/act/2025/17/eng@2025-10-21
Doxing	Malicious publication of private identifying information such as home addresses or telephone numbers to incite real-world harassment.	May bypass the Data Protection Act's (DPA) legitimate interest clauses; and there is no standalone doxing offence. DPA link: https://www.odpc.go.ke/wp-content/uploads/2024/02/TheDataProtectionAct__No24of2019.pdf
Non-Consensual Intimate Imagery (NCII)	Distribution of private sexual images to humiliate or extort. The most common precursor to documented femicide cases.	Section 37 of the CMCA is operative; however, related harassment provisions under Section 27 suspended by High Court, October 2025 i.e., in the case of Reuben Kigame Lichete & Kenya Human Rights Commission (KHRC) vs. The Attorney General & Others (HCCRPET/E673/2025).
Gendered Disinformation	Coordinated campaigns using false narratives to silence women in public life, particularly women politicians and journalists.	No standalone offence; this directly undermines the Maputo Protocol's guarantee of women's right to political participation. Maputo Protocol link: https://au.int/en/treaties/protocol-african-charter-human-and-peoples-rights-rights-women-africa
AI-Enabled Abuse: Deepfakes and Voice Cloning	Use of generative AI to create synthetic sexual imagery or impersonate women's voices. 98% of all deepfake content globally is non-consensual sexual imagery targeting women.	No provision in any current Kenyan statute resulting in an absolute regulatory void.
Economic Tech-Abuse	Coercive control of Mpesa credentials, unauthorized digital loans, and mobile money monitoring as instruments of intimate partner control.	Not recognized as a distinct form of abuse in financial regulation; there is no reporting or remedy pathway.

1.4.2 The Permanent Record and Digital Trauma:

Unlike physical violence, digital violence is characterized by permanence. Once harmful content is uploaded, it becomes what this gap analysis terms a digital tattoo i.e., a state of perpetual victimization in which the original violation is continuously re-experienced for as long as the content remains accessible, leading to most women and girls from withdrawing from digital engagement. This in turn leads to reduced representation of women's voices in public debate, shrinking civic space, the weakening of inclusive governance, and the normalization of online misogyny through reduced counter-speech.

TFGBV must be recognized not merely as a digital version of offline abuse, but as a distinct, systemic violation of human rights that leverages the internet's unique affordances, namely speed, permanence, and anonymity, to create a borderless environment of harm. This aligns with the findings of the ACHPR Resolution 522, which calls on African states to recognize that digital violence is as damaging as physical violence and requires specific, gender-responsive legal remedies.

Whilst this gap analysis prioritizes women and girls due to the disproportionate and sexualized nature of digital harms they face, often orchestrated within a "manosphere" that weaponizes algorithms to silence women, it acknowledges that strengthening digital justice frameworks inherently benefits all genders. By confronting the systemic misogyny and "red pill" ideologies that normalize cyber-violations, we address the most acute failures in our current safety standards, thereby dismantling the patriarchal stigmas that often prevent Kenyan men and boys from seeking recourse. Ultimately, creating a robust, accountable "Silicon Savannah" ensures that any survivor, regardless of gender, can seek justice without fear of ridicule or further harm.

1.5 THE MACRO - ECONOMIC DIMENSION: TFGBV As A Structural Economic Crisis

TFGBV is not only a human rights and public health crisis. It is a structural economic crisis with measurable and growing macroeconomic consequences that affect the productivity, competitiveness, and human capital of Kenya's economy as a whole. Thus, framing TFGBV exclusively in human rights terms, while accurate and important, obscures its economic dimensions in ways that can limit political will for the investment required to address it comprehensively.

1.5.1 The Cost of Radio Silencing to Kenya's Knowledge Economy:

The UN Women Africa report of November 2025[18] documents that up to 60% of women leaders, journalists, activists, and students have reduced or abandoned their digital participation as a protective response to TFGBV. Each of these withdrawals represents not only a personal loss but an economic extraction, reducing the productivity, innovation, and leadership contribution of women who are critical participants in the knowledge sectors on which Kenya's digital economic aspirations depend.

The Association of Media Women in Kenya documented in 2024 that over 60% of women journalists in Kenya have experienced online violence [19]. When journalists self-censor beats relating to corruption, governance, and accountability, the consequent reduction in investigative journalism capacity is itself an economic harm, and corruption that goes unreported is corruption that persists, with documented economic costs in reduced investor confidence, misallocated public resources, and distorted market competition.

1.5.2 Economic TFGBV: Mobile Money, Fintech, and Digital Financial Exclusion:

Kenya's celebrated mobile money infrastructure, which achieved 91% penetration and reshaped global financial inclusion discourse, has simultaneously created new vectors of economic technology-facilitated abuse. **A 2024 collaborative regional audit by the Johns Hopkins Center for Global Women's Health and Gender Equity, the University of Nairobi WEE Hub, and UNFPA Kenya found that 31.1% of women reported technology-enabled economic abuse by partners, including control over phone access and MPesa credentials** [20]**.** This form of economic TFGBV includes coercive control of women's mobile money access, monitoring or interception of digital financial transactions, the misuse of digital loan platforms to impose unauthorized debts, and the use of mobile financial services to perpetrate fraud and extortion targeting women.

As Kenya operationalizes **the Virtual Asset Service Providers Act 2025**[21] and integrates emerging digital financial services into its broader economic framework, the risk surface for technology-facilitated economic abuse will expand significantly.

Current regulatory frameworks, including the **Draft Virtual Asset Service Providers Regulations 2026**[22] and the Non-Deposit Taking **Credit Providers Regulations 2025**[23]**,** focus on anti-money laundering and institutional stability but lack explicit safeguards against technology-enabled financial coercion. The Central Bank of Kenya's Consumer Protection Framework must be amended to formally recognize digital financial coercion, including forced disclosure of M-Pesa or digital wallet credentials, as a specific form of economic abuse, mandating that licensees implement safety triggers for suspicious transaction patterns and establish gender-sensitive reporting and remedy pathways.

[18] *https://africa.unwomen.org/en/16DaysofActivism2025WCA*
[19] *https://amwik.org/wp-content/uploads/2025/03/AMWIK-TFGBV-RESEARCH-2024-1.pdf*
[20] *https://kenya.unfpa.org/sites/default/files/pub-pdf/tf_gbv_report_web_1.pdf*
[21] *https://new.kenyalaw.org/akn/ke/act/2025/20/eng@2025-11-04*
[22] *https://www.centralbank.go.ke/2026/03/18/public-notice-invitation-for-comments-from-the-public-on-the-draft-virtual-asset-service-providers-regulations-2026/*
[23] *https://www.centralbank.go.ke/2025/08/07/draft-non-deposit-taking-credit-providers-ndtcps-regulations-2025/*

1.5.3 The Demographic Dividend at Risk:

Kenya's development projections depend on the realization of a demographic dividend through the productive economic participation of a young, digitally connected population. TFGBV structurally compromises this dividend in two ways. First, by driving young women who constitute both the fastest-growing segment of the digital population and a critical component of the knowledge economy workforce out of digital participation and into economic precarity through the reputational, employment, and educational consequences of targeted digital abuse. Second, by normalizing misogynistic attitudes and behaviours among young men through algorithmic exposure to manosphere content, creating a cohort of current and future workers, managers, and civic leaders with attitudes toward women that are harmful and economically dysfunctional in a knowledge economy that depends on collaborative, diverse, and psychologically safe workplaces. Addressing TFGBV is therefore not a gender equality initiative that competes with economic development for limited public resources. It is a precondition of the economic development Kenya is attempting to achieve.

1.6 SCOPE AND PURPOSE OF THIS INTERVENTION

This strategic intervention adopts a feminist, rights-based, and anticipatory governance approach. It seeks to map Kenya's existing legal, regulatory, and institutional frameworks addressing TFGBV; identify gaps, inconsistencies, and enforcement failures; integrate insights from survivors and frontline practitioners; and develop evidence-based, survivor-centred, and forward-looking recommendations for legal and policy reform.

Guided by a Pan-African feminist theory of change, this work recognizes TFGBV as a structural manifestation of gender inequality requiring holistic, transformative responses that integrate feminist legal reform, institutional accountability, platform governance, and survivor-centred justice.

This gap analysis adopts what it terms a Future-Back methodology that entails framing Kenya's legal and policy response not against the harms that current statutes were designed to address, but against the foreseeable trajectory of technological change that will define the harm landscape of the next decade. This approach is essential because Kenya's regulatory architecture, designed for a pre-generative AI, pre-deepfake environment, is already structurally behind the harm frontier. The question this analysis asks is not only how to fix the framework for the present, but how to build a framework resilient enough to govern an AI-enabled future.

Whilst TFGBV targets individuals of all genders, including men and boys who may face cyber bullying, identity theft or digital fraud, this gap analysis focuses on women and girls, who are disproportionately subjected to more severe, frequent, and sexualized forms of digital harm. However, it is critical to recognize that any positive strides made to effectively address and combat TFGBV against women and girls will inherently empower boys and men as well.

In Kenya's patriarchal social context, men and boys are often less protected by existing frameworks and may hesitate to report digital violations for fear of ridicule or perceived weakness. Strengthening the overall digital justice system therefore creates a safer environment for all survivors to seek recourse without the barriers of social stigma.

This gap analysis recognizes that TFGBV harms are often systematically orchestrated within the manosphere, a digital ecosystem of misogynistic communities that weaponize algorithms to amplify coordinated campaigns targeting women in public and professional life. By centering this demographic, the analysis addresses the most acute failure of current digital safety frameworks and confronts the manosphere's role in normalizing the radio silencing of women, working toward a truly inclusive and accountable Silicon Savannah.

CHAPTER 2.
REVIEW OF EXISTING LEGAL AND POLICY FRAMEWORKS : GAPS AND REQUIRED AMENDMENTS

Kenya's legal architecture relevant to TFGBV draws from multiple statutory instruments, none of which was designed with a comprehensive, gender-responsive framework for technology-facilitated harm in mind. This section maps the principal instruments requiring the most urgent reform, identifies the specific gaps, explains why amendments are necessary, and proposes concrete reform pathways, while benchmarking Kenya's legal response against relevant regional and international frameworks.

It focuses in detail on the Computer Misuse and Cybercrimes Act, the Data Protection Act, the Sexual Offences Act, the Kenya Information and Communications Act, and the Artificial Intelligence Bill, with the remaining domestic instruments and applicable international frameworks presented in consolidated reference tables for ease of reference.

DOMESTIC LEGAL INSTRUMENTS

2.1 THE COMPUTER MISUSE AND CYBERCRIMES ACT (CMCA) 2018, AS AMENDED 2024 AND 2025

The CMCA remains Kenya's primary cybercrime statute[24] and the most directly applicable instrument to TFGBV. Section 27 criminalises cyber harassment; Section 37 addresses non-consensual sharing of intimate images. **The 2024 Amendment Act**[25] increased penalties for cyber harassment to a maximum of ten years' imprisonment or a fine of twenty million Kenya shillings and expanded definitional scope; **the 2025 Amendment Act**[26] introduced SIM-swap fraud provisions under Section 42A and an expanded phishing definition.

A judicial intervention of foundational consequence has, however, materially altered the Act's operational force. On 22 October 2025, the High Court suspended enforcement of Section 27(1)(b), Section 27(1)(c), and Section 27(2), following a constitutional petition by the Kenya Human Rights Commission and others (HCCRPET/E673/2025), on grounds of overbreadth, vagueness, and disproportionate infringement of the Article 33 right to freedom of expression. The conservatory orders remain in force pending final constitutional determination. The practical effect is that the enhanced penalties and expanded definitions introduced by the 2024 and 2025 Amendments, the very provisions designed to close the TFGBV enforcement gap are currently unenforceable. Kenya is returned to the narrower 2018 provisions for criminal harassment cases, while Section 37, Section 42A, and the phishing provisions remain operative.

The identified gaps are structural and cumulative because the Act contains no gender-responsive definition of TFGBV, treating cyber harassment as a generic offence that fails to capture its systemic, coordinated, and structurally gendered character. The suspension has created a critical enforcement vacuum of uncertain duration. Neither the original Act nor the amendments contain any provision governing AI-generated deepfake sexual imagery, albeit globally, 98% of deepfake video content constitutes non-consensual intimate imagery (NCII), of which 99% targets women, as documented by **Security Hero in 2023**[27] and confirmed by the **European Parliamentary Research Service in 2025**[28]**,** yet the creation of synthetic intimate imagery remains entirely unpunished in law.

UNODC's 2025 Global Strategy on Technology-Facilitated Gender-Based Violence, as presented at the NCII Abuse Summit in New York[29]**,** underscores that the absence of rapid takedown mechanisms is a critical systemic gap, noting that it transforms NCII from a discrete incident of abuse into a sustained form of coercion and control. Given the

[24] *https://new.kenyalaw.org/akn/ke/act/2018/5/eng%402022-12-31*
[25] *https://www.parliament.go.ke/sites/default/files/2024-09/THE%20COMPUTER%20MISUSE%20AND%20CYBERCRIME%20%28AMENDMENT%29%20BILL%2C2024.pdf*
[26] *https://new.kenyalaw.org/akn/ke/act/2018/5/eng@2025-11-04*
[27] *https://www.securityhero.io/state-of-deepfakes/*
[28] *https://ceeddw.org/wp-content/uploads/2025/05/NCII_DeepFakes_ThreatsRecommendations.pdf*
[29] *https://www.unodc.org/unodc/en/ngos/leaders-gathered-at-the-ncii-abuse-summit-to-tackle-technology-facilitated-gender-based-violence.html*

persistence and replicability of online content, harm is not limited to initial publication but continues, and often escalates, for as long as the material remains accessible, rendering frameworks without emergency removal powers insufficient for effective survivor protection.

Within this context, Section 37 of the CMCA does not establish a dedicated NCII-specific enforcement regime and remains primarily structured around general offence creation rather than survivor-centred remedies. It does not provide an express statutory framework for emergency takedown orders, expedited data preservation obligations, or a tailored interim injunctive relief mechanism for the rapid removal of non-consensual intimate imagery. Whilst courts may still grant preservation or removal orders through general constitutional and procedural jurisdiction, the Act itself does not codify a streamlined, survivor-initiated administrative pathway for time-sensitive content suppression, thereby relying on broader judicial and investigative processes rather than a specialised NCII response system.

In parallel, institutional reforms within the national cybercrime coordination architecture have strengthened reporting and escalation pathways for harmful online content. **These developments facilitate more structured coordination for content removal requests through the National Computer and Cybercrimes Coordination Committee (NC4), including submission via its official reporting channels**[30], although operational takedown authority remains exercised within the broader statutory and inter-agency framework rather than as an autonomous statutory power.

More broadly, the CMCA retains a predominantly punitive architecture focused on detection, prosecution, and sanctioning of offenders, without an integrated survivor protection and recovery framework. It does not provide a comprehensive statutory regime for digital content erasure or restoration orders, nor does it establish a dedicated compensation mechanism for victims of technology-facilitated abuse. Whilst broader legal remedies may be available under constitutional and civil law principles, these are not systematised within the Act as specialised, technology-specific safeguards.

With respect to financially motivated sextortion and similar cyber-enabled crimes, enforcement challenges persist in relation to cryptocurrency and other virtual asset ecosystems. Although general asset tracing, freezing, and forfeiture mechanisms exist under Kenya's broader criminal justice and anti-money laundering framework, the CMCA itself does not contain specific provisions tailored to virtual asset tracing or recovery in cybercrime contexts. This creates practical enforcement constraints in addressing cross-border, digitally mediated financial crime, particularly where anonymity-enhancing technologies are used.

The constitutional suspension is not merely a procedural complication but a structural design failure reflecting a recurring Kenyan legislative pattern of drafting in broad, vague terms that prioritise expansive deterrence over constitutional precision. The lesson is not that robust TFGBV legislation is constitutionally impermissible; it is that such legislation must be drafted with scrupulous attention to proportionality, necessity, and legality from the outset, engaging comprehensively with **the ACHPR Guidelines on Freedom of Expression**[31]**.**

Required amendments to the CMCA to enable it more effectively combat TFGBV include a comprehensive standalone TFGBV chapter with a gender-responsive, constitutionally precise definition; constitutionally compliant redraft of Section 27 incorporating ACHPR proportionality principles; explicit criminalisation of the creation and distribution of AI-generated non-consensual sexual imagery; a dedicated NCII offence regime; a statutory emergency takedown mechanism enforceable against ISPs and platforms within defined timelines; a survivor-centred recovery framework including digital erasure orders and compensation; aggravated penalty provisions for cryptocurrency-facilitated sextortion and coordinated attacks on women in public life.

2.2 THE DATA PROTECTION ACT (DPA) 2019

The DPA[32] establishes a technically competent and internationally aligned framework for the protection of personal data, creating the Office of the Data Protection Commissioner (ODPC) with powers to investigate complaints, issue enforcement notices, and impose administrative penalties. Its gender-neutral drafting reflects a global legislative standard and is not, in principle, a defect. The problem is the practical consequence of applying a gender-neutral instrument to a category of harm that is, by its nature, structurally gendered. The result is a functional blindness within the Act's architecture: an inability to see, name, or respond to the specific, escalatory, and often lethal ways in which personal data is weaponized against women and girls.

[30] *https://nc4.go.ke/*
[31] *https://www.chr.up.ac.za/images/researchunits/dgdr/documents/ati/Declaration_of_Principles_on_Freedom_of_Expression_ENG_2019.pdf*
[32] *https://www.odpc.go.ke/data-protection-laws-kenya/*

A data protection framework that treats the non-consensual publication of a woman's intimate images for purposes of sexual extortion with the same legal tools and procedural timelines as an unauthorised marketing email is not a framework calibrated to the reality of the harm it is being asked to address. The Data Protection Act (DPA) as currently drafted cannot see this distinction, and because it cannot see it, it cannot respond to it with the urgency, specificity, and protective force that TFGBV survivors require.

Moreover, in documented cases in Kenya, as evidenced by the National Police Service (NPS) data and statistics tabled before the Senate in May 2025, a record 578 femicide cases were reported in 2024, a significant increase from the 535 cases recorded in 2023[33]. These figures, are corroborated by **the 2025 Silencing Women Report[34],** which reveals that approximately 70% of these killings were perpetrated by intimate partners or family members, with victims aged 18 to 35 being disproportionately targeted. Critically, many of these physical acts were preceded by documented patterns of online harassment and coercive digital control, establishing a direct and evidenced continuum between data weaponization and fatal physical harm that the DPA's current architecture cannot interrupt.

The Act's structural inadequacies compound this failure across four specific dimensions.

First, the ODPC has no mandate to prioritize TFGBV complaints above routine commercial data disputes and no emergency powers to compel immediate content takedown. The standard procedural timelines for erasure under Section 40 are measured in weeks and months; the window within which content removal can meaningfully limit ongoing harm is measured in hours. This temporal incompatibility cannot be resolved through administrative efficiency. It requires a fundamentally different legal instrument operative on a crisis timescale.

Second, the enforcement mandate gap is self-perpetuating, because without a specific TFGBV mandate there is no dedicated capacity; without capacity there is no disaggregated data; without data there is no institutional accountability; and without accountability there is no structural pressure for reform.

Third, survivors are routinely referred between the DCI for criminal investigation and the ODPC for privacy complaints with no integrated referral pathway, no single point of contact, and no statutory coordination protocol between these bodies or the ODPP and Policare.

Fourth, platforms operating in Kenya face no explicit digital safety obligations under the Act beyond general data processing requirements, leaving algorithmic amplification of harmful content and failures of content moderation entirely outside the ODPC's regulatory scope.

The amendments required to enable the DPA to function effectively as a component of Kenya's TFGBV response architecture are specific and achievable. They are: aggravated harm provisions establishing an elevated category of data violation for TFGBV conduct, with enhanced penalties and accelerated investigation timelines calibrated to the severity and gendered targeting of the violation; emergency content removal powers operative within hours of a verified TFGBV complaint rather than at the conclusion of standard administrative processes; mandatory safety by design obligations on data controllers operating social media platforms, online communication services, and digital dating applications with Kenyan users; a statutory coordination protocol establishing integrated referral and case management between the ODPC, the DCI, the ODPP, and Policare; and heightened protection provisions for data held in intimate partner contexts, including emergency account access restoration and device surveillance detection assistance as specific data protection remedies available to survivors of digital coercive control.

2.3 THE SEXUAL OFFENCES ACT NO. 3 OF 2006 (SOA)

The SOA[35] establishes Kenya's core sexual violence offences but was enacted to address physical acts and reflects the legal understanding of harm dominant at the time of drafting. Its principal offences require physical contact or proximity, rendering them inapplicable to forms of digital or technology-facilitated sexual violence where harm is severe but no physical touch occurs.

AI-generated non-consensual sexual imagery, virtual sexual harassment, and deepfake sexual abuse fall entirely outside the Act's definitional scope. There is no recognition of technology-mediated sexual violence, no AI-specific consent framework, and no mechanism for assessing the non-consensual use of a person's likeness in synthetic content. The failure to recognise digital sexual violence as equivalent in gravity to physical sexual violence, which constitutes a structural gap in women's protection that reflects and perpetuates the legal invisibility of online harm.

The amendments required to enable the SOA to function effectively in combating TFGBV include an extension of its

[33] *https://www.odpc.go.ke/data-protection-laws-kenya/*
[34] *https://www.youtube.com/watch?v=VZMhjEJns78*
[35] *https://femicide.africauncensored.online/*

definitional framework to cover technology-facilitated sexual offences, explicitly including non-consensual creation or distribution of sexual imagery regardless of whether physical contact occurred; virtual sexual harassment causing psychological harm equivalent to physical sexual assault; and sextortion carried out through digital means. Additionally, a technology-facilitated sexual offences schedule should be added as an annex.

2.4 THE KENYA INFORMATION AND COMMUNICATIONS ACT (KICA) 2013

KICA[36] establishes the mandate of the Communications Authority of Kenya and provides the foundational architecture for telecommunications and internet service provider regulation. Its generational mismatch with the current digital environment is the source of a regulatory gap that is not simply a gap in coverage, but rather a gap in leverage.

Global platforms have developed a clear operational preference for formal judicial orders over administrative regulatory notices, treating the latter as legally soft and subject to their own policy discretion. KICA provides the Communications Authority with institutional foundation but without the specific, enforceable instruments required to compel compliance from global technology companies on TFGBV matters.

Google's Global Transparency Report of February 2026 records that Google rejected nearly 62% of content removal requests submitted by the Kenyan government in the first half of 2025[37]**.** In TFGBV contexts, this compliance failure is not an administrative inconvenience, rather it is a fundamental denial of survivor protection. When a major platform determines that a takedown request is insufficiently justified under its global policy framework, a survivor of non-consensual intimate image abuse is left in a condition of perpetual, compounding harm whilst the regulatory system nominally designed to protect her is effectively ignored.

KICA's broad safe harbour protections insulate platforms from liability for content generated by users, premised on an understanding of platforms as passive conduits that no longer reflects their role as active architects of content distribution whose algorithmic decisions determine what is amplified and rendered visible. Platforms operating in Kenya are not required to maintain localized, gender-sensitive content moderation in Swahili or the cultural registers through which Kenyan TFGBV is predominantly perpetrated, creating a structurally inferior level of protection for Kenyan women, compared to users in Global North jurisdictions.

The Ministry of Interior's administrative direction requiring platforms to establish local presence, **with META having complied and TikTok, X, and Telegram in the process of doing so is a meaningful development, but without statutory underpinning, it cannot create consistent binding obligations**[38]. The absence of a streamlined judicial pathway for Urgent Digital Protection Orders leaves the most acute category of legal need without an adequate mechanism.

To effectively combat technology-facilitated gender-based violence, KICA must be amended to include a statutory Urgent Digital Protection Order mechanism enabling ex parte applications with 24-hour compliance timelines for the most severe TFGBV content categories and revenue-calibrated automatic escalating financial penalties for non-compliance; conditional platform liability replacing broad safe harbour where platforms fail to respond to verified complaints or court orders, where their algorithms demonstrably amplified TFGBV content, or where feature design facilitated coercive control at scale; mandatory localized content moderation requirements for platforms with more than one million Kenyan users including Swahili-language moderation capacity and locally based trust and safety personnel; mandatory transparency reporting on TFGBV complaints disaggregated by content type, response time, and outcome; and data localisation requirements for evidence relevant to TFGBV investigations.

2.5 THE PROTECTION AGAINST DOMESTIC VIOLENCE ACT (PADVA) 2015

The PADVA[39] is among the most directly applicable yet least systematically utilized instruments for addressing TFGBV in intimate partner contexts. Its broad definition of domestic violence, which encompasses psychological, emotional, and economic abuse, intimidation, and harassment under Section 3, captures the spirit of coercive digital control. However, it does not name technology as a medium through which such violence can be perpetrated.

[36] *https://new.kenyalaw.org/akn/ke/act/1998/2/eng@2022-12-31*
[37] *https://weetracker.com/2026/02/12/kenya-google-takedow-rate/#:~:text=The%20company›s%20latest%20transparency%20report,stands%20far%20above%20global%20averages*
[38] *https://parliament.go.ke/node/25210*
[39] *https://www.kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ProtectionAgainstDomesticViolenceAct_2015.pdf*

Behaviours extensively documented in this gap analysis, including the installation of stalker ware, forced password sharing, social media monitoring, location tracking, and the use of intimate images as instruments of extortion, fall within the Act's definition in spirit but not in text, thus creating interpretive uncertainty for police officers, magistrates, and protection order applicants. Furthermore, there are no digital evidence standards for domestic violence proceedings, and no provision directing courts to treat patterns of digital coercive control as relevant risk factors when issuing, extending, or varying protection orders.

The PADVA should be amended to name technology-facilitated domestic abuse as a specific category within its definition of domestic violence; to require courts to consider digital coercive control in protection order assessments; and to mandate that orders issued include provisions prohibiting a respondent from accessing or monitoring a complainant's digital accounts, devices, or communications. These amendments are critical because the intimate partner relationship is the primary site of technology-facilitated coercive control for the majority of women in Kenya, and the PADVA, as the most accessible civil remedy available to survivors, is the most efficient instrument through which rapid digital protection can be provided without the evidentiary threshold required for criminal prosecution.

2.6 THE CHILDREN ACT, 2022

The Children Act of 2022[40] consolidates Kenya's child protection framework, with Section 23 protecting children from all forms of abuse and Section 24 imposing obligations on state and duty-bearers to prevent, investigate, and respond to child abuse. However, the Act does not explicitly recognize technology-facilitated abuse as a named category of child harm. Online grooming, exposure to harmful content through algorithmic recommendation, digital peer abuse including the circulation of intimate images between minors, and exploitation of children through digital platforms by adult predators all fall outside the Act's definitional scope, creating the same interpretive uncertainty identified in the analysis of the Protection Against Domestic Violence Act.

The Act equally fails to address the specific harms arising from the deployment of AI-driven digital learning tools and behavioural data collection systems in Kenyan schools under the Competency Based Curriculum (CBC), and establishes no parental rights to information about how children's behavioural and learning data is collected and used by digital platforms operating within the educational system.

The Children Act should be amended to explicitly recognize technology-facilitated child abuse as a specific and named category within its definition of abuse; to impose child safety obligations on digital platform operators whose services are directed at or foreseeably used by children, including content moderation, age verification, parental consent mechanisms, and accessible reporting tools; and to establish the rights of parents and guardians to receive full disclosure of data collection practices affecting their children in any institution or platform operating under state authorization.

These obligations are consistent with Kenya's constitutional obligations under Article 53 and with **the Convention on the Rights of the Child (CRC)**[41] to which Kenya is a party, and with **General Comment No. 25 of the Committee on the Rights of the Child**[42]**,** which provides the authoritative international standard for the application of CRC obligations in digital environments.

2.7 THE ARTIFICIAL INTELLIGENCE BILL, 2026: A CRITICAL ASSESSMENT

The Artificial Intelligence Bill of 2026[43]**,** sponsored by Nominated Senator Karen Nyamu and currently before the Senate, represents Kenya's most significant legislative attempt to date to govern artificial intelligence. It criminalizes deepfake-generated content, adopts a risk-based regulatory model aligned with the **European Union's Artificial Intelligence Act**[44], and requires the Advisory Committee on AI to be gender-balanced. As a signal that Kenya's legislature recognizes AI-enabled gender harm as a governance priority requiring statutory intervention, the Bill is a meaningful and welcome starting point.

However, in its current form it is not viable as an effective instrument for addressing TFGBV and requires significant amendment before enactment.

[40] *https://judiciary.go.ke/download/the-children-act-2022/*
[41] *https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child*
[42] *https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation*
[43] *https://new.kenyalaw.org/akn/ke/bill/senate/2026-02-19/the-artificial-intelligence-bill-2026/eng@2026-02-19*
[44] *https://artificialintelligenceact.eu/*

The proposal to establish three entirely new regulatory bodies, an AI Commissioner, an AI Authority, and an Advisory Council, alongside the existing Office of the Data Protection Commissioner and the Communications Authority, creates parallel regulatory structures with undefined jurisdictional boundaries and no integration with the DCI or NC4. For a TFGBV survivor who has experienced AI-generated intimate image abuse, this architecture risks requiring simultaneous navigation of multiple oversight bodies with no integrated referral pathway, compounding the institutional fragmentation this gap analysis identifies as one of the foundational failures of Kenya's current TFGBV response. The Bill also lacks gender-specific provisions despite its origins and the risk classification framework does not identify AI systems generating non-consensual sexual imagery as prohibited risk applications, and there are no provisions addressing model poisoning, prompt injection attacks on survivor support systems, or the particular compliance burden imposed on Kenyan developers who adapt pre-trained open-source models rather than building AI from scratch.

Despite these shortcomings, the Bill's risk classification framework, regulatory sandboxes, transparency requirements, and criminal penalties for misuse contain the building blocks of an effective regime.

What is required is targeted amendment rather than rejection that includes designating the AI Commissioner as a coordinating body operating through existing institutional mandates; explicitly classifying AI systems generating non-consensual sexual imagery as prohibited risk applications; introducing dedicated children's AI protection provisions; incorporating electoral AI disinformation provisions responsive to the 2027 General Election risk; and calibrating compliance obligations to distinguish between developers who build models from scratch, deployers who adapt pre-trained models, and operators who use them without modification. Approached in this way, the AI Bill 2026 can evolve from a promising but flawed first draft into the gender-responsive, institutionally coherent, and technically credible AI governance framework that Kenya's position as the Silicon Savannah demands.

CONSOLIDATED REFERENCE: ALL DOMESTIC INSTRUMENTS

The following table maps all seventeen domestic instruments identified in Chapter 2 against their primary gaps and the reforms required to constitute an adequate TFGBV legal architecture.

Instrument	Key Gaps	Required Reform
Constitution of Kenya (2010)	No explicit digital rights recognition	Judicial interpretive guidelines on digital dimensions of Arts 27, 28, 31
CMCA 2018 (as amended 2024/2025)	Enhanced harassment provisions (S.27) suspended Oct 2025; no AI/deepfake offences; no NCII regime; no takedown mechanism; no survivor remedies	Redraft S.27 constitutionally; standalone TFGBV chapter; criminalise AI-NCII creation; emergency takedown orders; survivor restitution; crypto/sextortion provisions
Data Protection Act (2019)	Gender-neutral; no aggravated harm category; standard erasure timelines incompatible with viral harm; no ODPC emergency powers; no platform safety obligations; no criminal-justice integration	Aggravated harm provisions; emergency erasure orders (hours not weeks); safety-by-design obligations; ODPC–DCI referral protocol; intimate-partner data protection category
Sexual Offences Act (2006)	Physical contact requirement excludes digital/AI sexual violence; no virtual sexual offence provisions; no AI consent framework	Extend definitions to technology-mediated offences; add technology-facilitated sexual offences schedule; virtual sexual violence equivalence
Penal Code (Cap. 63)	Criminal defamation constitutionally fragile; intimidation provisions predate digital threats	Update intimidation framework for online coordinated harassment
Evidence Act (Cap. 80)	No digital evidence protocols; inconsistent admissibility standards for screenshots, metadata, CDRs	Technology-specific amendments; mandatory collection/preservation protocols; platform-assisted evidence preservation; judicial training

Instrument	Key Gaps	Required Reform
KICA (2013)	62% government takedown requests rejected by platforms (Google, H1 2025); no mandatory localized moderation; broad safe harbour shields platforms; no Urgent Digital Protection Orders	Statutory Urgent Digital Protection Orders; conditional platform liability; mandatory localized moderation (Swahili); transparency reporting; revenue-calibrated penalties
PADVA (2015)	Digital coercive control (stalkerware, location tracking, NCII coercion) not named as domestic violence; no digital evidentiary standards in protection orders	Explicit technology-facilitated domestic abuse definition; courts to consider digital coercive control patterns in protection orders
Victim Protection Act (2014)	No TFGBV-specific protocols; no recognition of Digital Tattoo/Forced Occupational Trauma; framework ends at trial conclusion	TFGBV survivor category; digital harm assessment; content removal referral; ongoing post-trial protection standards
Counter-Trafficking Act (2010)	No technology-facilitated trafficking provisions; sextortion–trafficking nexus unrecognised	Online recruitment/grooming provisions; NC4/DCI/ODPC coordination; sextortion–trafficking prosecution guidelines
Children Act (2022)	Digital abuse not named; no platform child-safety obligations; no data rights for parents in educational AI contexts	Technology-facilitated child abuse definition; platform child-safety obligations; parental data rights in CBC digital tools
Employment Act (2007)	Digital workplace harassment excluded from S.6 sexual harassment definition; no employer obligations for digital conduct policies	Extend S.6 to electronic communications; mandatory digital conduct in harassment policies; NLRC digital harassment capacity
NCIA (2008)	Gender not a protected characteristic for hate speech; manosphere campaigns may not meet definitional threshold	Add gender as protected characteristic; extend hate speech to coordinated misogynistic digital campaigns; annual NCIC monitoring data
Media Council Act (2013)	No digital safety obligations on media houses; no journalist TFGBV recording mechanism	Digital safety policies mandatory; annual disaggregated journalist harassment data; NC4 coordination
NGEC Act (2011)	TFGBV absent from monitoring mandate; no disaggregated data obligations on state actors; no biennial TFGBV report	Explicit TFGBV monitoring mandate; compulsory data reporting by state actors; biennial TFGBV report
AI Bill (2026 – pending)	Three parallel new regulatory bodies create institutional fragmentation; no prohibited-risk classification for AI-NCII; no children's AI provisions; compliance burden miscalibrated for open-source developers	Replace parallel bodies with coordinating AI Commissioner within existing mandates; classify AI-NCII as prohibited; add children's and electoral AI provisions; tiered compliance for deployers vs developers

CONSOLIDATED REFERENCE: INTERNATIONAL AND REGIONAL FRAMEWORKS

Kenya has ratified or committed to a range of regional and international frameworks imposing explicit obligations with respect to TFGBV. The following table maps each instrument, Kenya's current legal status, and its direct relevance to the domestic reforms recommended in Chapter 2.

Instrument	Status	Kenya Position	Direct Relevance to TFGBV Reform
African Charter on Human and Peoples' Rights (1981) + ACHPR Guidelines 2019	Binding	Ratified	Arts 2, 3, 4, 5; ACHPR Guidelines affirm online VAW obligations consistent with free expression — must guide S.27 redrafting
Maputo Protocol + ACHPR Resolution 522 (2022)	Binding	Ratified	Arts 3 & 4; Resolution 522 explicitly requires specific digital violence legislation, dedicated institutions, and survivor redress — Kenya satisfies none comprehensively
AU Convention on Ending Violence Against Women & Girls (Feb 2025)	Binding	Member state — accession priority	First regional treaty expressly covering cyberspace violence; most current continental standard for CMCA/DPA/SOA amendments
CEDAW + GR No. 35 (2017)	Binding	Ratified	GR 35 recognises TFGBV as gender discrimination; requires accessible, effective laws; maps directly onto VPA, Employment Act, and CMCA gaps
Budapest Convention on Cybercrime	Binding	Accession approved	MLA frameworks, 24/7 contact points, e-evidence preservation — requires Evidence Act and CMCA alignment
Malabo Convention (AU Cyber Security & Data Protection)	Binding	Accession approved	Continental data protection standards support DPA amendments; NC4 and DCI must meet institutional requirements
ILO Convention 190 (2019) + Recommendation 206	Binding on ratification	Not yet ratified — priority advocacy	First international labour standard covering technology-facilitated workplace harassment; ratification would compel Employment Act S.6 amendments
CRC (1989) + General Comment No. 25 (2021	Binding	Ratified	GC 25 addresses children's digital rights, online grooming, algorithmic profiling; authoritative standard for Children Act and AI Bill children's provisions
UN Declaration on Elimination of VAW (1993) + Special Rapporteur	Persuasive / politically binding	Endorsed	Foundational state obligation framework; Special Rapporteur country observations set evidentiary and institutional benchmarks
SDGs 5 & 16	Political commitment	Committed (Vision 2030)	SDG 5 targets elimination of all forms of VAW including digital; SDG 16 requires access to justice — VNR mechanism available for accountability reporting
AU Agenda 2063 + Digital Transformation Strategy 2020–2030	Political commitment	Founding member	Gender equality as foundational AU development principle; TFGBV governance presented as precondition for digital inclusion commitments
Istanbul Convention (CoE, 2011)	Persuasive benchmark only	Non-party	International gold standard for VAW legislation; Art 17 (media self-regulation) and Art 50 (immediate law enforcement response) relevant as comparative drafting benchmark

Note: The Istanbul Convention (CoE, 2011) is included as a persuasive comparative benchmark only because Kenya is not a party to this instrument.

CHAPTER 3.
STAKEHOLDER CONSULTATION: ISSUES RAISED AND ANALYSIS

A multi-sectoral virtual stakeholder consultation was convened on 18 February 2026, bringing together representatives from state institutions, county gender offices, civil society organizations, feminist networks, women in media, women in politics, and academic institutions. The consultation was structured around a presentation by **the Gap Analysis Consultant, Mutheu Nyagah Khimulu**[45]**,** *followed by facilitated discussion that generated practice-grounded evidence on the nature, scope, and institutional response to TFGBV. In accordance with Kenya's Data Protection Act 2019 and the ethical protocols governing this consultancy, all contributions are treated as confidential and attributed to institutional roles only.*

3.1 THE EXPANDING TYPOLOGY OF TFGBV: Beyond Conventional Categories

Practitioners across all sectors documented forms of TFGBV that remain largely invisible in existing legal frameworks. The following categories each represent a gap in the current response architecture.

3.1.1 Coercive Digital Control in Intimate Relationships:

Multiple participants described the systematic use of digital tools within abusive intimate partner relationships, including the installation of spyware on partners' devices, forced password sharing, social media monitoring, hacking, and location tracking. A practitioner working on women's leadership and safety issues noted that these patterns are rarely named as violence, yet they fundamentally shape women's freedom, safety, and capacity for autonomous participation. A community organizer raised the specific concern that TFGBV mapping exercises must not exclude coercive digital control within intimate relationships simply because it occurs in the domestic sphere.

3.1.2 Workplace Digital Harassment:

A civil society representative highlighted workplace digital harassment as pervasive and systematically dismissed, including sexual messages transmitted on professional messaging platforms, late-night video call demands, and professional advancement conditioned on private digital communications. This conduct falls within the scope of workplace sexual harassment under the **Employment Act 2007**[46] but is rarely recognized or prosecuted as such. The Kenya Editors' Guild has publicly affirmed that the digital workplace constitutes a full extension of the professional workspace and that constitutional labour rights apply in their entirety to digital professional environments, a standard the statutory text does not yet reflect.

3.1.3 Cancel Culture as Political Censorship:

A practitioner in democratic governance identified the weaponization of coordinated cancel culture campaigns against women in political circles and public life as an underrated form of TFGBV. These campaigns delegitimize women's credibility and drive them from digital platforms, functioning as political censorship with material consequences for the women's leadership pipeline and civic engagement, particularly in the period approaching Kenya's 2027 General Election.

3.1.4 Surveillance of Activists and Journalists:

Surveillance of journalists and activists through social media monitoring was raised as a documented harm that limits freedom of expression and creates a chilling effect on accountability journalism. The risk that Kenya's National Digital ID system, currently under development, could become an instrument of state or intimate partner surveillance was specifically noted. The system could morph into a tool to track citizens' movements or resources if deployed without robust privacy safeguards. This concern demands proactive regulatory attention and explicit privacy provisions in the system's design architecture before deployment.

[45] *https://www.linkedin.com/in/mutheu-khimulu-law/*
[46] *https://www.kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/EmploymentAct_No11of2007.pdf*

3.1.5 TFGBV in Educational Platforms:

A representative from an international development organization documented the prevalence of TFGBV in digital learning environments, including school WhatsApp groups, university forums, and online class platforms, encompassing the circulation of intimate images, cyberbullying, sexual harassment in class chats, and exposure pages that disproportionately target girls. **Research published by the United Nations Population Fund found that 64.4% of female students surveyed in Nairobi's higher learning institutions had personally experienced online violence, nearly double the rate of their male peers[47].**

3.1.6 Intimate Image Abuse and the Lethal Continuum:

A practitioner in the women in media sector presented documented evidence from the Coast region of intimate image abuse used to extort money from women, citing a case in which digital abuse escalated to the murder of the victim. The perpetrator was subsequently arrested and charged, but a life had already been lost. This account illustrates the lethal continuum between TFGBV and physical femicide that underpins the urgency of this analysis. The same practitioner noted that evidence collection in TFGBV cases is fundamentally compromised by perpetrators' use of disappearing messages on encrypted platforms, a gap confirmed by a county-level practitioner who described an active case rendered un-prosecutable for precisely this reason.

3.1.7 AI-Generated Deepfakes and Electoral Risk:

Two practitioners working in public interest advocacy raised the escalating risk of AI-generated deepfakes, noting both the technical difficulty of distinguishing synthetic from authentic content and the acute political manipulation risk in Kenya's approaching electoral cycle. One practitioner noted that politically aligned networks and anonymous accounts increasingly use digital technology to target individuals who raise accountability concerns, and that generative AI will amplify this risk significantly in the 2027 election campaign period. **Kenya's mobile penetration rate of 149.4%, as recorded by the Communications Authority of Kenya, combined with limited digital literacy, creates conditions in which AI-enabled electoral TFGBV could materially influence political outcomes and silence women candidates[48].**

3.2 SYSTEMIC INSTITUTIONAL AND LEGAL CHALLENGES

3.2.1 The Absence of a Standalone TFGBV Definition in Law:

Practitioners across media, civil society, and legal sectors identified the foundational systemic gap i.e., there is no standalone law that clearly defines TFGBV, thereby creating confusion for survivors about how and where to report, hesitancy among police to classify incidents, and uncertainty among prosecutors and judicial officers about which charges to prefer. A documented instance from 2025 of a Magistrate being unable to ascertain the applicable law in an active TFGBV case was cited as evidence that this is not an exceptional failure, but the predictable and recurring consequence of a definitional vacuum that cascades through every stage of the justice chain.

3.2.2 Digital Evidence Collection Failures:

An active case rendered un-prosecutable by a perpetrator's use of disappearing messages on WhatsApp was cited by a county-level practitioner. Practitioners in media advocacy noted that police and prosecutors lack training on digital evidence collection, and that digital forensic tools are either unavailable or their importance insufficiently understood. Forensic evidence requirements were identified as a practical difficulty in charging TFGBV cases, with survivors often not knowing how or where to report, and institutions uncertain about applicable charges.

3.2.3 Public Awareness Deficits:

A gender officer from a county government and a civil society representative both identified limited public awareness of TFGBV and of available legal frameworks as a primary barrier. Most people do not recognize digital abuse as a form of gender-based violence, leading to systemic underreporting, weak data collection, and underdeveloped survivor support systems. This awareness deficit is self-perpetuating because, without reporting there is no data, without data there is no policy case, and without policy investment there is no awareness.

3.2.4 Platform Accountability Failures:

Practitioners called for structured engagement with technology platforms to ensure accountability, faster content removal, and transparent response mechanisms. The cross-border nature of online violence creates jurisdictional barriers

[47] *https://kenya.unfpa.org/en/news/new-study-reveals-extent-technology-facilitated-gender-based-violence-kenyas-higher-learning*
[48] *https://www.ca.go.ke/mobile-broadband-use-surges-smartphone-penetration-climbs-ca-report-shows*

to prosecution of offshore perpetrators. X (formerly Twitter) and Telegram were specifically identified as particularly problematic due to their high traffic volumes and limited content controls in the Kenyan context. **The KICTANet Online Gender-Based Violence Tracker was shared as a practical tool for monitoring and recording TFGBV cases that could be leveraged for national data aggregation[49].**

3.2.5 Insufficient Data Infrastructure:

A representative from a constitutional commission mandated to promote gender equality identified insufficient reliable data on TFGBV as a critical governance failure, noting the need for strengthened coordination between research institutions and state and non-state actors. This finding is consistent with the data gap analysis presented by **the National Gender and Equality Commission in its institutional mandate[50]** review.

3.3 GOVERNMENT CAPACITY AND ONGOING INITIATIVES

A representative from the National Computer and Cybercrimes Coordination Committee (NC4) confirmed that NC4 is in the advanced stages of developing a CMCA 2018 Rapid Reference Guide and Template Charge Sheet, to standardize how investigators and prosecutors handle digital threats including TFGBV.

The Ministry of Interior and National Administration has directed an assessment of the prevalence of non-consensual sharing of intimate images and related forms of digital sexual violence within Kenya's online ecosystem.

The government has approved accession to the **Budapest Convention[51]** and **Malabo Convention[52]** to allow cross-border investigation and is operationalizing cyber desks to enhance reporting visibility.

Additionally, the Ministry of Interior has required platforms to establish local presence in Kenya to facilitate takedown and coordination, with META having complied and TikTok, X, and Telegram in the process of doing so.

These developments represent meaningful institutional progress. However, as multiple stakeholders noted, operational capacity remains insufficient, coordination between institutions is fragmented, and the gap between policy commitments and frontline delivery remains wide. Gender officers at the county level continue to work without the technical tools, training, or budgetary resources required to effectively address TFGBV cases referred to them.

3.4 STAKEHOLDER RECOMMENDATIONS FOR REFORM.

The stakeholder consultations generated a convergent set of recommendations with the highest level of cross-sectoral agreement i.e.:

a. Creation of a formally gazetted, multi-sectoral a.national TFGBV coordination framework led by government but operational across all sectors.
b. Combining regulatory reform with cultural transformation and digital safety education across all levels of the education and community engagement system.
c. Development of a simplified TFGBV toolkit highlighting prevention and response mechanisms and referral pathways for dissemination through civil society, community health workers, and grassroots organizations.
d. Transformation of technology from a tool of harm to a tool of solution through survivor-facing platforms that create awareness, provide reporting mechanisms, and connect survivors to support.
e. Ensuring that technology-facilitated coercive control within intimate relationships is explicitly included in TFGBV legal definitions and institutional response frameworks, and is not excluded simply because it occurs in the private sphere.
f. Structured and binding engagement with technology platforms to secure commitments on content accountability, takedown timelines, and transparency in reporting mechanisms.

[49] *https://ogbv.kictanet.or.ke/feed*
[50] *https://ngeckenya.org/*
[51] *https://www.coe.int/en/web/cybercrime/the-budapest-convention*
[52] *https://au.int/en/treaties/african-union-convention-cyber-security-and-personal-data-protection*

CHAPTER 4.
KEY INFORMATION QUESTIONNAIRE ANALYSIS

Key Informant Questionnaires were administered in three streams: one targeting state actors and constitutional office holders; one targeting civil society organizations and feminist groups; and one directed to individuals who had personally experienced TFGBV, conducted in March 2026 at the Wangu Kanja Foundation office[53]. All responses are treated as confidential in accordance with Kenya's Data Protection Act 2019 and the WHO ethical guidelines for researching violence against women[54]. No individual respondent is identified by name.

4.1 STATE ACTORS AND CONSTITUTIONAL OFFICE HOLDERS

4.1.1 Definition and Institutional Approach to TFGBV:

Definitions offered ranged from the specific, including financially motivated sexual extortion and the use of digital platforms to harass, exploit, or control people, to the minimal, including addressed through prosecutions and treated as a form of GBV. At least one respondent characterized TFGBV simply as a form of GBV, reflecting a failure to recognize it as a distinct category of harm with specific evidentiary, institutional, and remedial requirements that differ materially from generic gender-based violence.

The absence of consensus among state actor respondents on the adequacy of the current legal framework is itself a critical governance finding. When prosecutors, investigators, and institutional representatives hold materially different views on whether the applicable law is sufficient, prosecution outcomes become dependent on the individual judgment of the officer or prosecutor handling a particular case rather than on a clear, shared, and consistently applied legal standard. This inconsistency benefits perpetrators who operate in the resulting ambiguity and is directly harmful to survivors seeking predictable access to justice.

4.1.2 Legal Framework Reliance:

All respondents cited the Computer Misuse and Cybercrimes Act as the primary legal instrument. Additional frameworks cited included the Data Protection Act, the Sexual Offences Act, the Children Act, the Counter-Trafficking in Persons Act, the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), the Maputo Protocol, and the Evidence Act. The diversity of instruments cited across respondents, without any single integrated framework, reflects and confirms the patchwork legal architecture identified in Chapter 2 of this analysis.

4.1.3 Adequacy of Existing Laws:

Responses were notably divided, reflecting genuine institutional disagreement. One respondent argued that the CMCA applies to any existing offence committed through technology, treating technology as an aggravating factor rather than as a site of qualitatively distinct harm. Three other respondents directly contradicted this position, noting that existing laws do not adequately cover deepfake pornography, AI-generated impersonation, or voice cloning; that offenders use encrypted platforms and anonymous accounts making prosecution extremely difficult; and that technology, especially AI, has outpaced the law.

4.1.4 Operational Challenges and Recommendations:

Operational challenges identified included: low reporting rates due to shame and self-blame; lack of trauma-informed handling at the point of reporting; cases settled through informal or clan-based negotiation with survivors pressured to withdraw, particularly in North Eastern Kenya; poor coordination between police, the Office of the Director of Public Prosecutions, and the Judiciary; donor dependency and limited county budgets hampering specialized TFGBV units; inadequate forensic capacity; and a general knowledge gap at all levels of the justice system. Inadequately trained prosecutors were identified as the single most significant operational constraint.

[53] *https://wangukanja.org/*
[54] *https://www.who.int/publications/i/item/9789241510189*

State actor respondents proposed the following reforms: a comprehensive statutory definition of TFGBV; Standard Operating Procedures integrating TFGBV into case management; template charge sheets and a Rapid Reference Guide; equipping the DCI laboratory with digital forensic tools; regular mandatory training for prosecutors and investigators; community sensitization campaigns; and training on cryptocurrency investigation.

4.2 CIVIL SOCIETY ORGANIZATIONS AND FEMINIST GROUPS

Substantive responses were received from grassroots organizations, community-based organizations, women's rights networks, and individual practitioners operating across multiple counties including Nairobi, the Coast, Homa Bay, Kisii, Kitui, and various rural constituencies.

4.2.1 Forms and Vulnerability Profiles:

Online harassment, cyberbullying, non-consensual sharing of intimate images, body shaming, and persistent unwanted digital sexual advances were identified by respondents with more sophisticated digital literacy and urban or semi-urban operational contexts. Respondents operating primarily in rural or grassroots contexts reported physical and sexual abuse as the most prevalent forms, with technology playing a less central but increasingly relevant facilitation role. This divergence underscores the importance of disaggregating TFGBV data by geography, socio-economic context, and population group.

Young women and girls were identified as particularly vulnerable due to high digital platform engagement and existing gender inequalities. Educated, independent, and publicly active women were identified as disproportionately targeted by coordinated smear campaigns, particularly in political contexts. Young mothers, women with limited economic independence, school dropouts, domestic workers, and women in impoverished rural communities were identified as facing acute vulnerability due to the convergence of economic precarity and limited access to legal information and recourse.

4.2.2 Barriers to Justice and Effectiveness of Reporting:

Barriers were consistent and convergent across all regions, reflecting a systemic rather than incidental pattern of exclusion. Financial barriers, including the cost of legal fees and medical reports required as evidence, were identified as primary obstacles. Stigma, shame, lack of awareness of legal rights, corruption within law enforcement and judicial processes, and cultural norms that normalize violence or pressure survivors into informal settlement processes were documented as significant structural barriers across multiple counties.

Community-based systems were identified as the most trusted and accessible reporting mechanisms for many survivors. Platform-based complaint mechanisms received mixed assessments: some respondents noted content removal within three working days, while others noted significant delays. Several respondents recommended a maximum response time of one working day for the most severe TFGBV content. No respondent characterized existing laws as fully survivor-centred in practice.

4.3 SURVIVORS OF TFGBV: DIRECT EXPERIENCE QUESTIONNAIRE ANALYSIS

The respondents participated in the survivor questionnaire, conducted at the Wangu Kanja Foundation office in March 2026. They provided written responses to eleven questions exploring their experiences of online harm, interactions with reporting and justice systems, and recommendations for reform. These responses represent the survivor voice at the centre of this gap analysis and provide the lived-experience foundation upon which all legislative and institutional reform recommendations must be grounded.

4.3.1 Respondent Demographics:

Age Bracket	Number of Respondents	Percentage of Sample
18 to 25 years	0	0%
26 to 35 years	5	50%
36 to 45 years	3	30%
46 to 55 years	2	20%
56 to 60 years	0	0%
Over 60 years	0	0%

The concentration of respondents in the 26 to 45 age band reflects both the age profile of active digital platform users in Kenya and the demographic group most consistently identified across all three questionnaire streams as bearing the highest burden of TFGBV.

4.3.2 Key Findings: Safety, Awareness, and Institutional Response:

67%	78%	67%	100%
Felt safe using online platforms before experiencing TFGBV	Did not know where to report or seek help at the time of the incident	Did not feel heard or supported when they reported	Confirmed online harm affected their digital participation and wellbeing

4.3.3 Sense of Safety Before and After the Experience:

The respondents were asked whether they felt safe using online platforms before experiencing TFGBV. Of the nine respondents who answered this question, six (67%) indicated that they had felt safe, and three (33%) indicated that they had not. One respondent elaborated that she had felt no harm in posting and expressing herself on social media. A clear majority of survivors approached digital platforms without a prior sense of threat or risk. This indicates that digital safety education cannot be directed solely at women who are already aware of potential danger. It must reach those who currently feel safe, and may therefore be most vulnerable to being caught off guard.

All respondents who answered the follow-up question (100%) confirmed that the online harm experienced had affected their sense of safety, participation, or wellbeing. One respondent permanently withdrew from a major social media platform. Another described becoming very reserved because of fear of re-experiencing TFGBV. A third described acquiring limits in her online behaviour, specifically avoiding posting personal content on social media. A fourth described being always cautious whenever posting anything on social media as an enduring consequence of the harm. The unanimity of this response confirms, from survivors' own testimony, the phenomenon of radio silencing documented throughout this gap analysis i.e., every respondent who experienced TFGBV modified, restricted, or withdrew from her digital participation as a direct consequence, constituting a measurable and personally experienced loss of digital freedom and civic voice.

4.3.3 Institutional Secondary Victimization

The majority of survivors who engaged with formal institutions, particularly police stations, experienced victim shaming, dismissal, or active hostility. Specific negative experiences documented included: constant victim shaming; a reporting experience at a police station characterized as being brushed off; active distortion by police of information shared by the survivor; and institutional revictimization at police gender desks, with instances of both male and female officers mocking complainants and making inappropriate, sexualized comments regarding intimate evidence.

The pattern of victim shaming, dismissal, and active hostility at police stations documented in the survivor responses is not evidence of individual officer misconduct. It is evidence of a structural and institutional failure to train, equip, and hold accountable the officers at the first point of contact in the justice chain for TFGBV survivors. Every survivor who is shamed, mocked, or dismissed at a police gender desk is a survivor who will not report again, who will not encourage others to report, and whose experience of institutional betrayal compounds the original harm. These are the predictable outcomes of a system that has not made trauma-informed, survivor-centred first response a mandatory, monitored, and enforced standard.

4.3.5 Support That Would Have Been Most Helpful:

Legal support, specifically the follow-through of existing cases and access to legal representation, was identified as a priority by multiple respondents, with several noting that cases are unacceptably slow to resolve. One respondent highlighted a significant systemic barrier to justice, noting that after reporting a case, her mobile device was seized by police for digital forensic analysis. More than a year later, the device had still not been returned, severely compromising her ability to communicate and earn a living. The financial strain of replacing the device, coupled with the loss of a primary work tool, led her to conclude that the cost of reporting, compounding her trauma with a loss of essential property, would make her hesitant to seek state intervention in the future.

Emotional and psychosocial support, including counselling, was identified as critical by multiple respondents, with one noting that this was needed to avoid depression and psychological trauma.

Digital safety awareness and capacity building were identified as both an immediate need for survivors and a preventive need for the broader community.

The convergence of legal, emotional, and digital safety needs within individual survivors' responses reflects the holistic, interconnected nature of TFGBV harm i.e., survivor support infrastructure must address all three dimensions concurrently, rather than treating each in isolation.

4.3.6 Changes in Technology Use and Online Self-Expression:

All respondents who answered this question (100%) confirmed that the experience had changed their digital behaviour. Elaborations included being very reserved because of fear of re-experiencing TFGBV; setting limits on what is posted, specifically avoiding sharing personal content; acquiring greater knowledge about social media safety practices; and increased general caution about all social media use.

The unanimity of this response provides direct survivor testimony for the radio silencing phenomenon that is one of the primary analytical frameworks of this gap analysis. Every single survivor confirmed that TFGBV had reduced, restricted, or fundamentally altered her digital participation. This is not a side-effect of digital harm. For many perpetrators, it is the intended outcome.

4.3.7 Platforms Most Identified as Problematic:

Seven specific platforms were identified as the most problematic as regards TFGBV: X (formerly Twitter), WhatsApp, the Facebook comments section, Instagram, TikTok, Telegram, and Snapchat. This finding is consistent with the platform accountability concerns raised by civil society respondents and with the specific identification of X and Telegram as high-risk platforms by practitioners in the stakeholder consultation.

4.3.8 Improvements Wanted from Institutions and Platforms:

Respondents' recommendations were substantive, specific, and convergent:

a. Faster access to justice through adequate resourcing of forensic laboratories to expedite case processing.
b. Enactment and enforcement of laws that hold perpetrators accountable and protect survivors.
c. Creation of more TFGBV gender desks and safe spaces, with digital inclusion in cybercrime laws.
d. Stronger institutional follow-up and case resolution by the legal system.
e. Police sensitization on GBV and TFGBV as a specific training requirement, with a national police curriculum on TFGBV.
f. Open community forums for people affected by TFGBV.
g. Policies requiring social media platforms to protect their users.

4.3.9 What Justice and Accountability Look Like - Survivor Perspectives:

Respondents described justice as: perpetrators being held accountable; survivors being supported and protected; harmful content being deleted and removed from circulation; cases being brought to transparent closure; and tougher penalties being enacted and enforced.

Several respondents were direct about the current reality, characterizing accountability as very poor, null and void in their communities, or non-existent at police stations. One respondent framed justice in the immediate and practical terms of getting videos removed from social media, the most urgent and personal form of relief available to a survivor of intimate image abuse.

In TFGBV cases justice and accountability seems impossible, but through resilience some individuals have been able to win cases and get justice, and there is a need to ensure more people receive the help to do so. (Survivor respondent, March 2026)

Lives and livelihoods are permanently damaged post-TFGBV. Survivors have had to literally restart life again with nothing in another part of the country for their own physical safety, having narrowly escaped community mob justice. (Survivor respondent, March 2026)

4.3.10 What Policymakers Need to Understand - Messages from Survivors:

The collective weight of the messages from survivors to policymakers is unambiguous:

a. Digital harassment must be treated with the same seriousness as physical sexual gender-based violence.
b. Extensive reforms are needed because implementation of existing policies is not in order, and adequate resource allocation by government is essential.
c. Handling of TFGBV cases should be domesticated at the ward level so that survivors do not have to travel far to access help.
d. Specific trained officers should be designated to handle TFGBV cases at dedicated desks.
e. More awareness must be created on handling various scenarios of TFGBV.
f. Survivors know what they need, they can articulate it with precision and clarity, and they are not being heard.

4.3.11 Cross-Cutting Findings from the Survivor Questionnaire:

Read as a body of evidence rather than a series of individual responses, the survivor questionnaire reveals four cross-cutting findings with direct implications for the reform agenda.

First, there is a near-universal awareness gap at the point of crisis: 78% of respondents did not know where to report or seek help when the harm occurred. This is not a gap about legislation. It is a gap about community-level awareness, accessible referral pathways, and survivor-facing communication that Kenya's current TFGBV architecture does not provide.

Second, institutional secondary victimization is a documented, systematic reality: the majority of survivors who engaged with formal institutions, particularly police stations, experienced victim shaming, dismissal, or active hostility. This demands immediate, mandatory, and monitored reform of first-responder protocols across all police stations in Kenya.

Third, the impact of TFGBV on digital participation is universal and immediate: every respondent modified, restricted, or withdrew from digital activity as a consequence of the harm experienced. This constitutes direct survivor testimony for the radio silencing phenomenon that this analysis identifies as a structural threat to Kenya's democratic and economic landscape.

Fourth, survivors have a clear, consistent, and coherent vision of what they need: legal follow-through, emotional and psychosocial support, digital safety knowledge, police sensitization, and content removal. These needs are neither unreasonable nor unfamiliar. They are simply unmet.

[45] *https://www.unodc.org/unodc/en/ngos/leaders-gathered-at-the-ncii-abuse-summit-to-tackle-technology-facilitated-gender-based-violence.html*
[46] *https://ict.go.ke/sites/default/files/2025-03/Kenya%20AI%20Strategy%202025%20-%202030.pdf*
[47] *https://www.parliament.go.ke/sites/default/files/2026-04/The%20Artificial%20Intelligence%20Bill%2C%202026%20%28Senate%20Bills%20No.4%20of%202025%29_0.pdf*

CHAPTER 5.
THEMATIC GAP ANALYSIS

Drawing on the legislative review in Chapter 2, the stakeholder consultation in Chapter 3, and the three questionnaire streams analysed in Chapter 4, this chapter presents an integrated thematic gap analysis organized across nine interconnected categories of systemic failure in Kenya's TFGBV response architecture.

5.1 DEFINITIONAL AND LEGISLATIVE GAPS.

The most foundational gap in Kenya's TFGBV response is the absence of a clear, gender-responsive, technology-specific legal definition of TFGBV. The current reliance on generic cybercrime and GBV frameworks creates definitional uncertainty that cascades through the entire justice chain: survivors do not know how to name and report their experience; police do not know how to classify incidents; prosecutors do not know which charges to prefer; and judicial officers are uncertain about applicable legal standards.

The constitutional suspension in October 2025 of key CMCA harassment provisions has widened the enforcement gap further. Emerging harms including AI-generated deepfakes, voice cloning, synthetic sexual imagery, sextortion via cryptocurrency, and coordinated misogynistic attacks are entirely outside the definitional scope of existing legislation. The European Parliamentary Research Service 2025 confirmed that 98% of all deepfake content constitutes non-consensual sexual imagery, 99% of which targets women and girls.

5.2 ENFORCEMENT AND EVIDENTIARY DEFICITS

Kenya's enforcement architecture is marked by acute digital forensic deficits that function as structural barriers to TFGBV accountability. Investigators lack the training, tools, and standardized protocols to collect and preserve digital evidence to prosecution standards. The use of encrypted platforms with disappearing messages by perpetrators effectively destroys evidence before it can be secured. Metadata, hashed evidence, call data records, and geolocation data are inconsistently collected and rarely presented in court-admissible format.

The DCI National Digital Forensic Laboratory currently lacks the specialized tools and adequate personnel required to manage the escalating volume of cases nationwide. This centralized infrastructure is insufficient to serve the entire country, and whilst the ideal long-term solution is a fully equipped digital forensic laboratory in every ward, an immediate strategic priority must be for county governments to ensure that at least one dedicated laboratory exists per county.

The systemic gap is compounded by the absence of mandatory evidence preservation obligations on digital platforms operating within Kenya, which places the entire evidentiary burden on the physical hardware of the survivor.

5.3 INSTITUTIONAL FRAGMENTATION AND COORDINATION FAILURES

Kenya's institutional architecture for TFGBV response is fragmented across multiple agencies with overlapping mandates and insufficient coordination mechanisms. Survivors of TFGBV involving data privacy violations may need to simultaneously engage the Directorate of Criminal Investigations, the Office of the Data Protection Commissioner, Policare, the Office of the Director of Public Prosecutions, and the Judiciary, without any integrated referral pathway, case management system, or single point of contact. There is no gazetted, multi-sectoral national TFGBV coordination framework, despite widespread recognition of its necessity across all consultation streams. County Gender Departments have limited technical capacity, inadequate budgets, and no formal integration into the national TFGBV response architecture.

5.4 SURVIVOR-CENTRED REMEDY GAPS

Kenya's TFGBV response architecture prioritizes criminal punishment of perpetrators over the immediate protection, recovery, and empowerment of survivors. There are no emergency content removal orders, no statutory right to be forgotten, no interim injunctive relief against ongoing digital harm, and no compensation framework for reputational, psychological, economic, and professional harm.

Even successful criminal prosecutions fail to address the continuing harm experienced by survivors whose intimate images, defamatory content, or AI-generated abuse material remains publicly accessible online, a condition the **UNODC's 2025 Global Strategy on TFGBV describes as digital shackling**[55]

5.5 EMERGING TECHNOLOGY GOVERNANCE VOIDS

Kenya's regulatory framework is structurally unprepared for AI-enabled TFGBV. The creation and distribution of deepfake sexual imagery, voice cloning for synthetic intimate audio, nudify application outputs, and AI-generated disinformation campaigns targeting women are entirely outside the scope of current legislation. **Moreover, Kenya's National AI Strategy 2025**[56] to 2030 does not address the gendered dimensions of AI risk. **The Artificial Intelligence Bill 2026**[57] requires substantial amendment before it can serve as an effective instrument including explicit classification of AI systems generating non-consensual sexual imagery as prohibited-risk applications; a dedicated children's AI protection chapter; integration with existing institutional mandates rather than creation of three parallel regulatory bodies; mandatory adversarial robustness testing; and electoral AI disinformation provisions.

5.6 SOCIO-CULTURAL AND AWARENESS GAPS

A structural and pervasive barrier to TFGBV prevention is the low level of awareness within communities, institutions, and the general public. Survivors frequently encounter advice from family members, community elders, or police officers to ignore harassment, log off, or toughen up, responses that entrench cycles of impunity and normalize digital misogyny. The psychosocial impact of TFGBV, including Forced Occupational Trauma and the permanent psychological harm created by the digital record of abuse, is insufficiently recognized within Kenya's healthcare and judicial systems.

5.7 CHILDREN AND MINORS: A CRITICAL AND CURRENTLY UNPROTECTED POPULATION

TFGBV against girls does not begin at adulthood. It begins in school, in digital learning platforms, peer messaging groups, and social media ecosystems that form the social infrastructure of Kenyan adolescence. The rollout of Kenya's Competency Based Curriculum(CBC) has been accompanied by the deployment of AI-driven digital learning tools in public schools without systematic parental awareness of how children's behavioural and learning data is being collected, processed, and potentially profiled.

Additionally, content recommendation algorithms expose children to harmful material. Girls are disproportionately targeted by recommendation systems that amplify body image content and sexualized material. Boys are disproportionately exposed to manosphere content that algorithmically normalizes misogynistic attitudes, creating a supply-side dynamic for future TFGBV.

5.8 DEMOGRAPHIC DISAGGREGATION: INTERSECTING VULNERABILITIES

A feminist and rights-based gap analysis must disaggregate vulnerability profiles. Women with disabilities face both disproportionate vulnerability to digital violence and disproportionate exclusion from reporting mechanisms and support systems. Reporting mechanisms are frequently inaccessible to women with visual, hearing, or cognitive disabilities. Elderly women represent an almost entirely invisible population in TFGBV discourse, yet face specific documented harms including social engineering, digital financial fraud, coercive control over mobile money by family members, and weaponization of digital platforms to facilitate property disinheritance of widows.

A comprehensive TFGBV framework must use gender-neutral drafting for protective provisions while incorporating gender-specific analysis of risk profiles, ensuring that women receive the targeted protection they require and that male victims are not structurally excluded from legal recourse.

[55] *https://www.unodc.org/unodc/en/ngos/leaders-gathered-at-the-ncii-abuse-summit-to-tackle-technology-facilitated-gender-based-violence.html*
[56] *https://ict.go.ke/sites/default/files/2025-03/Kenya%20AI%20Strategy%202025%20-%202030.pdf*
[57] *https://www.parliament.go.ke/sites/default/files/2026-04/The%20Artificial%20Intelligence%20Bill%2C%202026%20%28Senate%20Bills%20No.4%20of%202025%29_0.pdf(*

5.9 THE VULNERABILITY MATRIX

The following matrix summarizes the distinct TFGBV risk profiles, AI-specific vulnerability dimensions, and key legal gaps across the demographic groups identified in this analysis.

Demographic Group	Primary TFGBV Risk Vectors	AI-Specific Vulnerability	Key Legal and Policy Gap
Girls in school (under 18)	NCII in peer groups, cyberbullying, grooming, educational data harvesting	CBC AI tools collecting data without consent; harmful content recommendation	No child-specific AI protections in AI Bill; no CBC digital data governance framework
Adolescent girls and young women (18 to 25)	Sextortion, deepfake sexual imagery, coordinated harassment, dating platform abuse	AI-generated synthetic sexual imagery; automated harassment bots; algorithmic amplification	No criminalisation of deepfake NCII creation; no platform liability for algorithmic amplification
Women in public life and media	Coordinated smear campaigns, deepfake imagery, doxing, impersonation, cancel culture	AI-generated electoral disinformation; voice cloning; gendered algorithmic shadow banning	No electoral AI disinformation provisions; no aggravated penalties for targeting women in public life
Women in intimate relationships	Digital coercive control, stalkerware, forced password sharing, economic tech-abuse	AI-powered surveillance tools; location tracking; AI financial fraud	No digital coercive control offence; no economic TFGBV provisions in financial regulation
Women with disabilities	Exploitation of limited digital literacy, inaccessible reporting mechanisms, cognitive manipulation	AI systems exploiting cognitive vulnerabilities; inaccessible reporting tools	TFGBV systems not disability-accessible; AI Bill has no disability-inclusive design requirement
Elderly women	Digital financial fraud, mobile money coercion, property disinheritance via digital means	AI-powered financial scams; deepfakes used for exploitation	No economic TFGBV provisions; no age-responsive digital literacy programme
Rural women of all ages	Economic tech-abuse, limited awareness, phone and Mobile money access controlled by partners	AI systems in language barriers; limited AI literacy; financial product targeting	Rural TFGBV not disaggregated in national data; no rural-responsive awareness programme
Men and boys	NCII fraud, impersonation, algorithmic radicalisation as secondary victims and future perpetrators	Manosphere content recommendation pipelines; AI-generated false evidence in domestic disputes	TFGBV framework should protect all persons; supply-side manosphere prevention not addressed

5.10 THE MANOSPHERE AND ALGORITHMIC AMPLIFICATION

A comprehensive TFGBV gap analysis must address not only the forms and impacts of digital violence, but the ecosystems and economic incentives that produce and perpetuate it.

The manosphere is a transnational digital ecosystem of misogynistic online communities that systematically produces and distributes content dehumanizing women, normalizing coercive control in intimate relationships, and coordinating targeted harassment campaigns[58]. Its Kenyan manifestations include coordinated political harassment campaigns targeting women aspirants and elected leaders, cancel culture campaigns against women in civic life, and the algorithmic exposure of Kenyan adolescent boys to content normalizing entitlement and contempt for women's agency.

The business models of major social media platforms are structurally misaligned with TFGBV prevention because, platforms monetize engagement, and their algorithmic systems demonstrably amplify content that provokes strong emotional responses.

[58] https://gnet-research.org/

CHAPTER 6.
EMERGING RISKS AND ANTICIPATORY ANALYSIS.

The Future-Back methodology adopted by this Project requires explicit attention to foreseeable risks arising from the intersection of technological change, political dynamics, and institutional inertia.

Kenya's digital policy decisions made today will determine the terrain on which TFGBV either escalates or is effectively addressed across the next decade.

This chapter identifies seven specific emerging risk categories, analyses their mechanisms, and provides the analytical basis for the anticipatory reform recommendations in Chapter 7.

6.1 AI-ENABLED ESCALATION AND THE DEEPFAKE CRISIS

AI-generated deepfake sexual imagery is the fastest-growing form of digital gender-based violence globally. As generative AI tools become more accessible, cheaper, and easier to use without technical expertise, the volume and quality of deepfake content will increase dramatically. Kenya's legal framework has no capacity to address the creation, distribution, or possession of AI-generated non-consensual intimate imagery. In the specific context of Kenya's 2027 electoral cycle, the combination of deepfake technology with Kenya's mobile penetration rate of 149.4% and limited digital literacy creates conditions in which AI-enabled electoral TFGBV could materially influence political outcomes and silence women candidates.

6.2 DIGITAL ID SYSTEMS AND SURVEILLANCE RISK

Kenya's National Digital ID system, currently under development, presents significant risks if deployed without robust privacy safeguards and democratic accountability mechanisms. The system could enable the tracking and monitoring of individuals' movements, resources, and communications in ways that could be weaponized as instruments of both state and intimate partner surveillance. The use of digital ID to locate and monitor survivors who have fled abusive intimate partners requires explicit privacy safeguards built into the system's design architecture before deployment, not retrofitted after harm has occurred.

6.3 PLATFORM ACCOUNTABILITY AND THE GOVERNANCE GAP

Social media platforms including TikTok, X, and Telegram continue to operate without full local presence in Kenya, albeit in the process of setting up local offices, limiting law enforcement's ability to enforce takedown orders, obtain user data, and hold platforms accountable. Google's **Global Transparency Report of February 2026**[59] recorded that Kenya's government content removal requests were rejected at a rate of approximately 62% in the first half of 2025. This figure provides quantitative evidence of the platform compliance gap that formal statutory obligations must address.

6.4 CRYPTOCURRENCY-FACILITATED TFGBV

The use of cryptocurrency to fund and facilitate cross-border sextortion, child sexual abuse material production, and other forms of TFGBV represents an emerging and rapidly escalating threat. State actor respondents specifically identified cryptocurrency as a financing mechanism for organized criminal TFGBV that the current legal framework cannot address. As cryptocurrency adoption in Kenya increases, driven in part by mobile money integration and the country's fintech innovation ecosystem, chain analysis capacity and the legal framework to trace, freeze, and confiscate cryptocurrency proceeds of TFGBV become essential infrastructure requirements.

59https://transparencyreport.google.com/

6.5 THE DIGITAL LITERACY DIVIDE AND INTERGENERATIONAL RISK

The intergenerational and rural-urban digital literacy divide creates asymmetric vulnerability profiles across Kenya's demographic landscape. Research from **Johns Hopkins Bloomberg School of Public Health (2024)**[60] found that 31.1% of women in regional audits reported technology-enabled economic abuse by partners, including control over phone access and M-Pesa credentials. Young urban women face deepfake, sextortion, and coordinated harassment risks, whilst rural women face tech-enabled intimate partner control and mobile money coercion. An effective TFGBV prevention framework must therefore be tailored to these divergent vulnerability profiles.

6.6 QUANTUM COMPUTING: THE LONG-TERM THREAT TO DIGITAL EVIDENCE INTEGRITY

Quantum computing represents an imminent and existential threat to Kenya's digital evidence architecture and to the cryptographic protocols currently securing survivors, witnesses, and investigators in TFGBV cases. The most acute near-term danger is the harvest now, decrypt later threat: sophisticated criminal syndicates and state-level actors are already intercepting and storing encrypted communications and digital evidence from high-stakes investigations, with the strategic intent to decrypt this data as soon as quantum capacity matures commercially. This means that evidence collected today using current encryption standards may be vulnerable to future decryption, rendering today's confidentiality guarantees retroactively void.

The legal admissibility frameworks currently being developed for digital evidence in Kenya must be designed from the outset to incorporate post-quantum cryptographic standards, aligned with the **National Institute of Standards and Technology's post-quantum cryptographic standards finalized in 2024**[61]**.** All DCI laboratory investments, all evidence preservation protocols developed under recommended Evidence Act amendments, and all survivor data repositories established under the recommended national TFGBV coordination framework must be built with post-quantum resilience as a mandatory baseline specification from inception.

6.7 AI CYBERSECURITY THREAT VECTORS: MODEL POISONING AND PROMPT INJECTION

The Artificial Intelligence Bill 2026 does not address AI-specific cybersecurity threat vectors. Model poisoning, in which a malicious actor corrupts the training data or parameters of an AI system to cause systematically biased or harmful outputs, poses a particular threat to AI-powered content moderation systems.

A poisoned moderation model could systematically fail to detect TFGBV content while appearing to function normally, enabling harm at scale behind a facade of platform compliance.

Prompt injection attacks, which exploit the ability to manipulate an AI system's behaviour by embedding adversarial instructions within input data, have direct relevance for AI-powered survivor support chatbots and government AI tools, where attackers could redirect survivors away from reporting mechanisms, extract identifying information, or produce responses that minimize experiences of violence.

Mandatory adversarial robustness testing should be required for all high-risk AI systems deployed in Kenya's justice, health, and social services contexts.

[60] *https://publichealth.jhu.edu/sites/default/files/2025-10/Agile-2.0-2024-Women-s-Data-County-Specific-Dissemination-Brief-BUNGOMA.pdf*
[61] *https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-cryptography-standards*

CHAPTER 7
RECOMMENDATIONS AND WAY FOWARD

The following recommendations are presented across nine thematic areas. They are grounded in the evidence generated through the legislative review, stakeholder consultation, and three questionnaire streams of this analysis, and are also guided by feminist legal principles and survivor-centred justice, and are designed to be practically achievable within Kenya's constitutional, institutional, and resource context, whilst remaining responsive to future technological change.

7.1 LEGISLATIVE REFORMS

7.1.1 Enact a Standalone Technology-Facilitated Gender-Based Violence Act:

Kenya requires a standalone, comprehensive TFGBV Act providing a gender-responsive definition of TFGBV; criminalizing the full spectrum of TFGBV including AI-generated non-consensual intimate imagery, deepfakes, voice cloning, sextortion, doxing, coordinated harassment, and coercive digital control in intimate relationships; establishing emergency content removal orders enforceable against social media platforms and online service providers; creating a survivor-centred recovery mechanism including compensation for reputational, economic, and psychological harm; and mandating a National TFGBV Action Plan.

The **UN Women Model Framework for Legislation on Technology-Facilitated Violence Against Women and Girls (2025)**[62] should inform the drafting process, alongside ACHPR Resolution 522 on the **Protection of Women Against Digital Violence in Africa**[63] and the **AU Convention on Ending Violence Against Women and Girls adopted in February 2025.**[64]

7.1.2 Urgently Redraft the Suspended CMCA Provisions:

The constitutional suspension of Section 27(1)(b), Section 27(1)(c), and Section 27(2) of the Computer Misuse and Cybercrimes Act has created an enforcement vacuum requiring immediate legislative response. The suspended provisions must be redrafted in constitutionally compliant terms addressing the court's concerns regarding overbreadth and vagueness, drawing on the **ACHPR Guidelines on Freedom of Expression and Access to Information in Africa**[65] to ensure the balance between harm prevention and expression protection is properly calibrated in statute.

The redrafted provisions should also introduce: explicit criminalisation of AI-generated non-consensual intimate imagery; a dedicated NCII offence framework; platform liability for failure to remove TFGBV content within mandated timelines; aggravated offence provisions for cryptocurrency-facilitated TFGBV; and a survivor-centred recovery mechanism.

7.1.3 Amend the Data Protection Act, the Sexual Offences Act, PADVA, and KICA:

The Data Protection Act 2019 requires amendment to introduce aggravated harm provisions for the weaponization of personal data; ensure emergency erasure and content removal powers exercisable within hours of a verified TFGBV complaint; mandate safety by design obligations on social media platforms; and establish statutory integration with criminal justice referral mechanisms.

The Sexual Offences Act should be amended to extend its definitional framework to virtual and technology-mediated sexual offences, including AI-generated non-consensual sexual imagery and digital sexual coercion.

[62] *https://www.unwomen.org/en/digital-library/publications/2025/11/brief-model-framework-for-legislation-on-technology-facilitated-violence-against-women-and-girls*
[63] *https://achpr.au.int/en/adopted-resolutions/522-resolution-protection-women-against-digital-violence-africa-achpr*
[64] *https://au.int/en/treaties/african-union-convention-ending-violence-against-women-and-girls*
[65] *https://achpr.au.int/en/soft-law/guidelines-freedom-expression-and-access-information-africa(*

The Protection Against Domestic Violence Act 2015 should be amended to include explicit recognition of technology-facilitated domestic abuse as a named category within its definition of domestic violence.

The Kenya Information and Communications Act 2013 should be amended to introduce a statutory Urgent Digital Protection Order mechanism enabling expedited judicial orders with twenty-four-hour compliance timelines enforceable against platforms regardless of country of incorporation; conditional platform liability for TFGBV-enabling conduct; mandatory localized content moderation for platforms with more than one million Kenyan users; and mandatory transparency reporting obligations.

7.1.4 Amend Related Domestic Instruments:

The Employment Act 2007 should be amended to explicitly extend its sexual harassment provisions to digital workplace conduct.

The Children Act 2022 should be amended to explicitly recognize technology-facilitated child abuse and impose child safety obligations on digital platform operators.

The National Cohesion and Integration Act 2008 should be amended to include gender as a protected characteristic in its hate speech provisions.

The National Gender and Equality Commission Act 2011 should be amended to include TFGBV explicitly within the Commission's monitoring and investigation mandate.

7.2 INSTITUTIONAL STRENGTHENING

A gazetted, multi-sectoral national TFGBV coordination framework should be established with a clear mandate, defined membership spanning NC4, the ODPC, the National Police Service, the ODPP, the Judiciary, county gender departments, and civil society organizations, and an annual public accountability reporting requirement. Additionally, a national TFGBV data collection and reporting standard should be developed and made mandatory across all participating institutions.

The DCI laboratory requires urgent investment in digital forensic tools and specialist capacity, with post-quantum resilience as a mandatory design requirement. Furthermore, mandatory digital forensic training for cybercrime investigators should be established with specific modules on TFGBV evidence collection, cryptocurrency tracing, and AI-generated content analysis.

The ODPP should establish specialized TFGBV prosecution units with dedicated trained prosecutors and updated Decision to Charge Guidelines specifically addressing TFGBV charging decisions.

County Gender Departments require dedicated budgetary allocations, technical training, and formal integration into national TFGBV coordination pathways. Gender Technical Working Groups at county level should be formally institutionalized and resourced. Gender Desks at police stations should receive TFGBV-specific training, standardized protocols, and regular monitoring to end victim shaming and establish trauma-informed first response as a non-negotiable standard.

7.3 PLATFORM ACCOUNTABILITY

The government should accelerate the requirement for all major social media platforms to establish local presence in Kenya.

Binding platform safety obligations should be introduced through the KICA amendment recommended above, including: enforceable content removal timelines; financial penalties for non-compliance calibrated to platform revenue; and mandatory gender-disaggregated algorithmic impact assessments. Kenya should engage proactively with international platform governance frameworks including the **EU Digital Services Act framework**[66], to advocate for global adoption of Safety by Design standards as a mandatory baseline for AI systems.

[51] *https://www.unwomen.org/en/digital-library/publications/2025/11/brief-model-framework-for-legislation-on-technology-facilitated-violence-against-women-and-girls*
[52] *https://achpr.au.int/en/adopted-resolutions/522-resolution-protection-women-against-digital-violence-africa-achpr*
[53] *https://au.int/en/treaties/african-union-convention-ending-violence-against-women-and-girls*
[54] *https://achpr.au.int/en/soft-law/guidelines-freedom-expression-and-access-information-africa*
[66] *https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package*

7.4 SURVIVOR SUPPORT INFRASTRUCTURE

A comprehensive survivor support infrastructure requires: the elimination of financial barriers to accessing justice in TFGBV cases through dedicated legal aid; the establishment of safe houses in every sub-county as critical protection infrastructure; integration of TFGBV-specific psychosocial support services into existing GBV referral pathways; development of a simplified TFGBV toolkit and referral guide for dissemination through civil society organizations, community-based organizations, and community health workers; operationalization of the KICTANet Online GBV Tracker as a national data aggregation and case monitoring tool; and development of economic empowerment support for TFGBV survivors whose livelihoods have been permanently damaged, including vocational retraining and transitional financial assistance.

7.5 DATA, RESEARCH, AND ACCOUNTABILITY

The government should mandate national TFGBV data collection standards integrated across law enforcement, the Judiciary, health, and social services, with mandatory disaggregation by gender, age, disability status, rural or urban residence, and economic status.

Additionally, a national TFGBV data observatory should be supported in collaboration with research institutions and civil society. The NGEC should be specifically empowered to publish a biennial TFGBV report. The findings of the Ministry of Interior's assessment of the prevalence of non-consensual sharing of intimate images should be published and integrated into the legislative reform process.

7.6 INTERNATIONAL COOPERATION AND ALIGNMENT

Kenya should prioritize the full operationalization of its accession to the Budapest Convention on Cybercrime and the Malabo Convention, developing domestic legal frameworks to give effect to mutual legal assistance, extradition, and cross-border investigation provisions.

Furthermore, Kenya should also ratify **ILO Convention 190 on Violence and Harassment (2019)**[67] as a priority advocacy commitment. Kenya's treaty body reporting to CEDAW and the African Commission should explicitly address TFGBV, and the government should engage proactively with ACHPR Resolution 522 implementation monitoring mechanisms.

7.7 CHILDREN AND MINORS: SPECIFIC AI AND TFGBV PROTECTIONS

The Artificial Intelligence Bill 2026 must be amended before enactment to include a dedicated children's AI protection chapter prohibiting the profiling of persons under eighteen for commercial purposes; the deployment of AI systems designed to manipulate children's behaviour or beliefs; the collection of children's biometric or behavioural data without explicit, informed parental consent; and the deployment of high-risk AI systems in educational settings without a prior child rights impact assessment, parental notification, and a meaningful opt-out mechanism.

The Ministry of Education should be designated as the primary regulatory authority for AI systems deployed within the Competency Based Curriculum, exercising its oversight function in coordination with the Office of the Data Protection Commissioner, NC4, and the Communications Authority, each of which already holds statutory mandates directly applicable to the data protection, cybercrime, and communications dimensions of AI deployment in educational settings.

This approach delivers comprehensive, sector-specific oversight of AI in schools without creating an additional regulatory layer, without imposing further compliance complexity on institutions seeking redress for AI-enabled harm, and without adding to the public expenditure burden of establishing a new commission.

A dedicated digital safety curriculum should also be integrated into the CBC at all levels, covering age-appropriate digital rights literacy and gender-responsive content on consent and online safety.

[55] *https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package*
[67] *https://www.ilo.org/dyn/normlex/en/f?p=NORMLEXPUB:12100:0::NO::P12100_ILO_CODE:C190*

7.8 ADDRESSING THE ARTIFICIAL INTELLIGENCE BILL 2026: Integrated Recommendations

The AI Bill 2026 should be amended in the following specific respects before enactment.

a. Designate the AI Commissioner as a coordinating body operating through existing institutional mandates rather than parallel to them, with statutory interoperability obligations to the ODPC, NC4, the National Police Service, and the Communications Authority, and a single integrated TFGBV-AI complaint pathway.
b. Amend the risk classification framework to explicitly classify as prohibited or unacceptable risk any AI system designed to generate non-consensual sexual imagery of identifiable persons; any system designed to impersonate real persons for purposes of harm; and content recommendation systems that algorithmically amplify gender-based abuse content.
c. Include mandatory adversarial robustness requirements, including model poisoning and prompt injection testing, for all high-risk AI systems deployed in Kenya's justice, health, and social services sectors.
d. Amend the compliance framework for open-source model deployers to impose proportionate, technically achievable obligations focused on use case and harm impact assessment, rather than audit trail requirements that developers of pre-built models cannot meet.
e. Introduce specific electoral AI provisions, including mandatory labelling of AI-generated political content and a prohibition on synthetic political impersonation content in the twelve months preceding a general election.
f. Ensure that criminal sanctions apply at the organizational level to platform operators and AI system deployers whose products enable TFGBV, creating accountability where commercial decisions are made rather than only where harm manifests.

7.9 SOCIO-ECONOMIC WELLBEING: CROSS-CUTTING RECOMMENDATIONS

TFGBV is not only a human rights crisis. It is also a macroeconomic crisis with measurable consequences for Kenya's knowledge economy, workforce participation, and demographic dividend. Research by the **Association of Media Women in Kenya found that over 60% of women journalists in Kenya have experienced online violence**. Addressing TFGBV is therefore a precondition of the economic development Kenya is attempting to achieve, and not a gender equality initiative in competition with it and ways to do this include:

The National Treasury should commission a macroeconomic impact assessment of TFGBV on Kenya's knowledge economy and demographic dividend, with findings incorporated into the Medium-Term Expenditure Framework.

The Central Bank of Kenya's consumer protection framework should be amended to explicitly recognize technology-facilitated economic abuse, including mobile money coercion and digital financial exclusion in intimate partner contexts, as forms of gender-based violence with dedicated reporting pathways and remedy mechanisms.

The AI Commissioner's mandate to promote AI literacy should be resourced and implemented with specific attention to elderly women, rural women, women with disabilities, and women in informal economy contexts, using community radio, faith-based organizations, and community-based organization networks as primary delivery channels.

Kenya should develop and adopt a National Digital Safety and TFGBV Prevention Strategy as a distinct policy instrument, with measurable targets and annual progress reporting to Parliament.

Economic empowerment and livelihood reconstruction must be integrated into the survivor support architecture as a programmatic priority, recognizing that TFGBV permanently damages livelihoods and that meaningful justice includes the material conditions necessary for survivors to rebuild their lives.

[68] *https://amwik.org/2024/01/01/how-amwik-is-supporting-women-against-diggital-violence/*

7.10 CONSOLIDATED REFORM PRIORITIES AT A GLANCE

The following table presents the consolidated legislative, institutional, and programmatic reform priorities in order of urgency, together with the responsible lead institution and the international framework anchoring each commitment.

No.	Reform Priority	Lead Institution	Timeframe	International Anchor
1	Redraft suspended CMCA Section 27 provisions in constitutionally compliant terms	Parliament / Attorney General	Immediate	ACHPR Resolution 522; Maputo Protocol
2	Enact standalone TFGBV Act with gender-responsive definition and emergency remedies	Parliament	Short term (12 months)	AU Convention on EVAWG; CEDAW GR 35
3	Amend DPA to introduce aggravated harm provisions and emergency ODPC powers	Parliament / ODPC	Short term (12 months)	Malabo Convention; Maputo Protocol
4	Amend Sexual Offences Act to cover technology-mediated sexual offences	Parliament	Short term (12 months)	CEDAW GR 35; Budapest Convention
5	Amend KICA to establish Urgent Digital Protection Orders and platform liability	Parliament / CA	Short term (12 months)	ACHPR Guidelines; AU EVAWG Convention
6	Amend AI Bill 2026 before enactment: prohibited-risk AI-NCII; children's chapter; electoral provisions	Senate / Parliament	Immediate (Bill before Senate)	CRC GC 25; EU AI Act benchmark
7	Establish gazetted national TFGBV coordination framework (NC4, ODPC, NPS, ODPP, Judiciary, counties)	Ministry of Interior	Short term (6 months)	ACHPR Resolution 522; SDG 16
8	Invest in DCI digital forensic capacity with county-level laboratories and post-quantum standards	DCI / National Treasury	Medium term (24 months)	Budapest Convention
9	Establish specialized TFGBV prosecution units within the ODPP	ODPP	Short term (12 months)	CEDAW GR 35; Maputo Protocol
10	Mandate trauma-informed first response training at all police stations	NPS / Inspector General	Immediate (administrative)	Victim Protection Act; Istanbul Convention benchmark
11	Eliminate financial barriers to justice; establish TFGBV legal aid	National Legal Aid Service	Short term (12 months)	CEDAW GR 35; SDG 16
12	Ratify ILO Convention 190 and amend Employment Act for digital workplace harassment	Parliament / Ministry of Labour	Medium term	ILO C190; SDG 8
13	Operationalize Budapest and Malabo Convention accession domestically	Attorney General / Ministry of ICT	Medium term (24 months)	Budapest; Malabo
14	Amend PADVA, Children Act, Employment Act, NCIA, and NGEC Act	Parliament	Medium term	CRC; Maputo Protocol; CEDAW
15	National Digital Safety and TFGBV Prevention Strategy with annual Parliamentary reporting	Ministry of ICT / NGEC	Medium term (24 months)	AU Digital Transformation Strategy; Agenda 2063

CONCLUSION.

Kenya stands at a pivotal moment because, the same digital infrastructure that positions the Silicon Savannah as a global innovation leader is being systematically weaponized to silence, harm, and exclude the women and girls on whose full participation that leadership depends.

This gap analysis has documented that failure in granular detail across fifteen domestic legal instruments, fourteen regional and international frameworks, nine categories of systemic failure, and the direct testimonies of survivors who described relocating for their physical safety, restarting their lives with nothing, and enduring years without justice or the removal of the content that destroyed their reputations and relationships.

These are not statistical abstractions. They are the measurable human cost of a legal and institutional architecture that was never designed to see, name, or respond to technology-facilitated gender-based violence as the serious, structural, and escalating crisis that it is.

The solutions are not beyond Kenya's institutional or legislative capacity. They are clearly evidenced, regionally and internationally grounded, and in several cases already in motion: NC4's Rapid Reference Guide, the Ministry of Interior's platform presence requirements, the government's accession to the Budapest and Malabo Conventions, and the Artificial Intelligence Bill's introduction to the Senate all demonstrate that the political and institutional will for reform exists.

What this analysis has demonstrated is that the pace, coherence, and survivor-centredness of that reform must now accelerate and deepen. The moment to act is not after the next femicide case preceded by digital abuse, not after the 2027 General Election demonstrates what AI-enabled gendered disinformation can do to women's political participation, and not after quantum computing renders today's forensic evidence irretrievably compromised. The moment to act is now, and the roadmap for doing so is contained within this report.

CRAWN Trust commends this analysis to Parliament, the Attorney General's Office, the Cabinet Secretary for Interior and National Administration, the Cabinet Secretary for Information, Communications and The Digital Economy, the Office of the Director of Public Prosecutions, the National Computer and Cybercrimes Coordination Committee, the Office of the Data Protection Commissioner, and all civil society and development partners committed to ensuring that Kenya's Silicon Savannah becomes a genuinely safe, inclusive, and transformative digital frontier for every woman and girl in Kenya.

LIST OF ACRONYMS AND ABBREVIATIONS

HOW TO USE THIS LIST:

This list provides a complete reference for all acronyms, abbreviations, legislative short titles, institutional names, and international framework references used in the Gap Analysis on Technology-Facilitated Gender-Based Violence Against Women and Girls in Kenya (April 2026). The entries are arranged in five thematic sections: Domestic Legislation; Kenyan Institutions and Bodies; International and Regional Frameworks; International Organisations; and Subject Matter Terms and Technical Concepts. Within each section, entries appear in alphabetical order. Where a term appears in more than one section, for example CBC appears both as a curriculum and as a subject matter reference, a cross-reference is provided. Where relevant, a contextual note in italics identifies the significance of the entry to the substantive analysis.

SECTION 1: DOMESTIC LEGISLATION AND LEGAL INSTRUMENTS

Includes Acts of Parliament, subsidiary legislation, and constitutional petition references cited in this gap analysis.

Domestic Legislation and Legal Instruments	
Acronym	*Full Title and Contextual Note*
Cap. 63	**Penal Code (Chapter 63 of the Laws of Kenya)** Contains general offences including criminal intimidation and malicious communication applicable in TFGBV contexts.
Cap. 80	**Evidence Act (Chapter 80 of the Laws of Kenya)** Governs admissibility of evidence in Kenyan courts; currently lacks technology-specific digital evidence standards.
CBC	**Competency Based Curriculum** Kenya's national school curriculum framework; rollout has introduced AI-driven digital learning tools in public schools without adequate data governance.
Children Act	**Children Act 2022** Revises and consolidates Kenya's child protection framework; does not currently contain specific provisions addressing technology-facilitated abuse of children.
CMCA	**Computer Misuse and Cybercrimes Act 2018** (as amended 2024 and 2025) Kenya's primary cybercrime statute and most directly applicable instrument to TFGBV. Key harassment provisions suspended by High Court, October 2025.
CTPA	**Counter-Trafficking in Persons Act 2010** Criminalises trafficking; does not currently contain provisions on technology-facilitated trafficking or online recruitment and grooming.
DPA	**Data Protection Act 2019** Establishes the framework for collection, processing and storage of personal data; creates the ODPC. Gender-neutral drafting produces functional gaps in TFGBV response.
Employment Act	**Employment Act 2007** Section 6 defines sexual harassment; does not explicitly extend to digital workplace communications.
KICA	**Kenya Information and Communications Act 2013** Primary instrument regulating the communications sector and establishing the mandate of the Communications Authority of Kenya.
NCIA	**National Cohesion and Integration Act 2008** Prohibits hate speech and discrimination; does not explicitly include gender as a protected characteristic in hate speech provisions.
NDTCP	**Non-Deposit Taking Credit Providers Regulations 2025** Governs non-bank lending; does not include safeguards against technology-enabled financial coercion of women.
NGEC Act	**National Gender and Equality Commission Act 2011** Establishes the NGEC; does not currently include TFGBV within the Commission's explicit monitoring mandate.
OSHA	**Occupational Safety and Health Act** Does not currently define digital professional environments or recognize TFGBV as a workplace hazard.
PADVA	**Protection Against Domestic Violence Act 2015** Defines domestic violence broadly; does not explicitly name technology-facilitated coercive control as a form of domestic violence.
SOA	**Sexual Offences Act No. 3 of 2006** Establishes core sexual violence offences; physical contact requirement renders it inapplicable to technology-mediated sexual violence.
VASP Act	**Virtual Asset Service Providers Act 2025** Governs virtual asset service providers in Kenya; regulatory framework does not include safeguards against cryptocurrency-facilitated TFGBV or sextortion.
VPA	**Victim Protection Act 2014** Establishes the Victim Protection Board; does not contain provisions specifically addressing TFGBV survivors or the Digital Tattoo phenomenon.

SECTION 2: KENYAN INSTITUTIONS, BODIES AND OFFICES

Includes state institutions, constitutional offices, regulatory bodies, law enforcement agencies, civil society organisations, and coordinating bodies operating within Kenya.

Kenyan Institutions, Bodies, and Offices	
Acronym	**Full Title and Contextual Note**
AG	**Attorney General of Kenya** Principal legal adviser to the Government; responsible for mutual legal assistance and treaty implementation.
CA	**Communications Authority of Kenya** Primary regulator of the communications sector; established under KICA. Responsible for licensing ISPs and setting content standards.
CBK	**Central Bank of Kenya** Issues consumer protection framework for financial institutions; framework requires amendment to recognize digital financial coercion as a form of GBV.
CRAWN Trust	**Community Advocacy and Awareness Trust** Non-governmental organization implementing the Safe Spaces, Strong Voices project; commissioning body of this gap analysis.
DCI	**Directorate of Criminal Investigations** Primary criminal investigation body in Kenya; operates the National Digital Forensic Laboratory. Identified as lacking adequate digital forensic tools and personnel.
NCIC	**National Cohesion and Integration Commission** Established under the NCIA; mandate historically focused on ethnic and political conflict rather than gendered hate speech.
NC4	**National Computer and Cybercrimes Coordination Committee** Multi-agency body coordinating Kenya's cybercrime response; developing a CMCA Rapid Reference Guide and Template Charge Sheet for TFGBV cases.
NGEC	**National Gender and Equality Commission** Constitutional commission under Article 59; mandate does not currently include explicit TFGBV monitoring obligations.
NPS	**National Police Service** Kenya's primary law enforcement body; also referred to as Policare. First point of contact for TFGBV survivors; subject to documented secondary victimization concerns.
ODPC	**Office of the Data Protection Commissioner** Principal regulatory body established under the DPA; lacks emergency powers and an explicit TFGBV mandate within its enabling framework.
ODPP	**Office of the Director of Public Prosecutions** Responsible for all criminal prosecutions in Kenya; identified as lacking specialist TFGBV prosecution capacity.
Policare	**National Police Service — Victim Support and Gender Desks** Operational wing of the NPS responsible for GBV and victim support functions; survivor questionnaire identified secondary victimization at police gender desks.

SECTION 3: INTERNATIONAL AND REGIONAL FRAMEWORKS

Includes binding treaties, regional conventions, protocols, general recommendations, and international development frameworks referenced in this gap analysis, together with bodies responsible for their monitoring and implementation.

International and Regional Frameworks	
Acronym	Full Title and Contextual Note
ACHPR	African Commission on Human and Peoples' Rights Monitors compliance with the African Charter on Human and Peoples' Rights; issued Resolution 522 on the Protection of Women Against Digital Violence in Africa (2022).
ACHPR Resolution 522	African Commission on Human and Peoples' Rights Resolution 522 on the Protection of Women Against Digital Violence in Africa (2022) Explicitly recognises digital violence as a human rights violation; affirms state obligations to prevent, investigate, punish, and provide remedies.
AU	African Union Continental body; adopted the Convention on Ending Violence Against Women and Girls in February 2025, the first regional treaty expressly covering cyberspace violence.
AU EVAWG Convention	African Union Convention on Ending Violence Against Women and Girls (adopted February 2025) First AU treaty to expressly address violence within cyberspace; establishes binding obligations on member states to adopt technology-facilitated violence legislation.
Budapest Convention	Council of Europe Convention on Cybercrime (2001) International treaty facilitating cross-border cybercrime investigation and prosecution; Kenya has approved accession. Requires domestic legislative alignment.
CEDAW	Convention on the Elimination of All Forms of Discrimination Against Women Core UN human rights treaty; General Recommendation No. 35 (2017) recognises online and technology-facilitated violence as a form of gender-based discrimination.
CRC	UN Convention on the Rights of the Child (1989) Kenya is a party; General Comment No. 25 (2021) addresses children's rights in the digital environment and provides the authoritative standard for child AI protection provisions.
EPRS	European Parliamentary Research Service Research body of the European Parliament; 2025 report confirmed that 98% of all deepfake content constitutes non-consensual sexual imagery targeting women.
EU	European Union the EU Artificial Intelligence Act (2024) and Digital Services Act are referenced as comparative benchmarks for Kenya's AI governance and platform accountability frameworks.
ILO	International Labour Organization Specialised UN agency; Convention 190 on Violence and Harassment (2019) is the first international labour standard covering technology-facilitated workplace harassment. Kenya has not yet ratified.
ILO C190	ILO Convention 190 on Violence and Harassment (2019) Defines violence and harassment to include acts via work-related communications enabled by technology; Recommendation 206 addresses digital workplace harassment policy.

International and Regional Frameworks	
IPU	Inter-Parliamentary Union International organisation of national parliaments; survey found 80% of women parliamentarians in Africa have faced psychological violence online.
Istanbul Convention	Council of Europe Convention on Preventing and Combating Violence Against Women and Domestic Violence (2011) International gold standard for comprehensive VAW legislative frameworks; referenced as a comparative persuasive benchmark only — Kenya is not a party.
Malabo Convention	African Union Convention on Cyber Security and Personal Data Protection Continental framework for cybercrime governance and data protection; Kenya has approved accession. Provides additional support for DPA amendments.
Maputo Protocol	Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa Guarantees women's rights to dignity, life, and integrity; protection extends to digital environments through ACHPR Resolution 522.
SDG	Sustainable Development Goal UN framework; SDG 5 (Gender Equality) targets elimination of all forms of VAW including digital; SDG 16 (Peace, Justice and Strong Institutions) requires access to justice for all.
UN	United Nations International organisation; the UN Special Rapporteur on Violence Against Women, UN Women, UNODC, UNESCO, UNFPA and UNICEF are all referenced in this analysis.
UN Declaration on EVAW	UN Declaration on the Elimination of Violence Against Women (1993) Foundational international instrument defining state obligations with respect to violence against women; applies to violence perpetrated through private digital platforms.

SECTION 4: INTERNATIONAL ORGANIZATIONS AND RESEARCH BODIES

Includes United Nations agencies, international civil society organisations, professional associations, and research bodies whose findings, reports, or frameworks are cited in this analysis.

International Organisations and Research Bodies	
Acronym	Full Title and Contextual Note
APC	Association for Progressive Communications International non-profit focused on digital rights; conceptualises TFGBV as a pattern of psychological, emotional, sexual, economic and reputational harm carried out through digital means.
AWDF	African Women's Development Fund Pan-African grant-making foundation; funding partner for the Safe Spaces, Strong Voices project implemented by CRAWN Trust.
CCGD	Centre for Child and Gender Development Research partner in the 2024 UNFPA study on TFGBV in Nairobi's higher learning institutions.
FeCoMo	Federation of Community Media Organisations African media federation; co-hosted the 2025 UNESCO-FeCoMo High-Level Roundtable that affirmed the digital sphere as an inseparable extension of the professional workspace.
IAWRT	International Association of Women in Radio and Television International professional body; describes the persistent digital targeting of women journalists as creating a permanent hostile digital work environment.
KICTANet	Kenya ICT Action Network Civil society organisation focused on ICT policy; operates the Online Gender-Based Violence (OGBV) Tracker shared during the February 2026 stakeholder consultation.
NIST	National Institute of Standards and Technology (United States) Finalised post-quantum cryptographic standards in 2024; these standards are referenced as the mandatory baseline for Kenya's digital evidence preservation architecture.
UNESCO	United Nations Educational, Scientific and Cultural Organization Specialised UN agency; 2025 report documented that 75% of women media workers experience digital abuse while performing their duties.
UNFPA	United Nations Population Fund UN agency; 2024 research confirmed that 64.4% of female students in Nairobi's higher learning institutions have personally experienced online violence.
UNODC	United Nations Office on Drugs and Crime UN office; 2025 Global Strategy on Technology-Facilitated Gender-Based Violence identifies the absence of rapid takedown mechanisms as a critical gap in national frameworks.
WEE Hub	Women's Economic Empowerment Hub (University of Nairobi) Research institution; partner in the 2024 Johns Hopkins and UNFPA Kenya regional audit on technology-enabled economic abuse.
WHO	World Health Organization Specialised UN health agency; WHO ethical guidelines for researching violence against women governed the confidential survivor questionnaire administered in March 2026.

SECTION 5: SUBJECT MATTER TERMS AND TECHNICAL CONCEPTS

Includes acronyms and abbreviated terms for subject matter concepts, technical terminology, and thematic categories used throughout this analysis.

NOTE ON TERMINOLOGY:

The terms TFGBV (Technology-Facilitated Gender-Based Violence) and OGBV (Online Gender-Based Violence) are both used in this analysis, reflecting the terminology adopted by different institutions and instruments. OGBV is the term used by KICTANet in its OGBV Tracker and appears in several stakeholder contributions. TFGBV is the broader analytical category adopted throughout the main body of this report as it encompasses both online and offline digital facilitation of gender-based violence. Both terms refer to the same spectrum of harm.

The terms Non-Consensual Intimate Imagery (NCII) and Non-Consensual Sharing of Intimate Images (also abbreviated NCII in some instruments) are used interchangeably in this analysis. Both refer to the creation, distribution or possession of intimate images of a person without their consent.

Subject Matter Terms and Technical Concepts	
Acronym	Full Title and Contextual Note
AA	Level AA — Web Content Accessibility Guidelines (WCAG) International accessibility standard; referenced as the minimum design requirement for all TFGBV survivor-facing digital systems to ensure accessibility for women with disabilities.
AI	Artificial Intelligence AI Bill 2026 is currently before the Senate; the analysis calls for significant amendment before enactment including prohibition of AI-NCII systems and children's data protections.
AI Bill	Artificial Intelligence Bill 2026 Bill currently before the Kenyan Senate; proposes risk-based AI governance modelled on the EU AI Act. Requires amendment to address TFGBV and children's protections.
AML	Anti-Money Laundering Financial crime prevention framework; VASP regulations focus on AML compliance but lack explicit safeguards against cryptocurrency-facilitated TFGBV and sextortion.
CBO	Community-Based Organisation Grassroots civil society organisation; identified in this analysis as a key delivery channel for the simplified TFGBV toolkit and referral guide.
CBC	Competency Based Curriculum See Domestic Legislation section above.
CSO	Civil Society Organisation Non-governmental organisations; nine CSO respondents participated in the key informant questionnaire stream.
DFS	Digital Financial Services Encompasses mobile money, digital lending and virtual asset platforms; creates expanded risk surface for economic TFGBV as adoption increases.
GBV	Gender-Based Violence Violence directed at an individual based on their gender; TFGBV is a specific category of GBV facilitated or amplified through digital technologies.
GPS	Global Positioning System Satellite-based location tracking technology; referenced in the context of stalkerware and coercive digital surveillance in intimate partner relationships.

Subject Matter Terms and Technical Concepts	
HCCRPET / E673 / 2025	High Court Constitutional Petition E673 of 2025 Petition by the Kenya Human Rights Commission and Reuben Kigame Lichete challenging the constitutionality of CMCA Section 27 enhanced provisions; conservatory orders issued 22 October 2025.
KHRC	Kenya Human Rights Commission Constitutional commission; co-petitioner in HCCRPET / E673 / 2025 challenging the suspension of enhanced CMCA cyber-harassment provisions.
LLM	Legum Magister (Master of Laws) Postgraduate law qualification; referenced in the credentials of the Gap Analysis Lead Consultant, Mutheu Nyagah Khimulu LLM, Cyber Security, Counter Terrorism and Crisis Management.
MLA	Mutual Legal Assistance International law enforcement cooperation mechanism; operationalisation of Budapest Convention MLA frameworks requires targeted amendments to the Evidence Act and CMCA.
NCII	Non-Consensual Intimate Imagery The creation, distribution or possession of intimate images of a person without their consent; Section 37 of the CMCA addresses sharing but lacks a dedicated offence framework with emergency remedies.
OGBV	Online Gender-Based Violence Terminology used by KICTANet for its OGBV Tracker; functionally equivalent to TFGBV in most contexts within this analysis.
PPE	Personal Protective Equipment Referenced in context of 'digital PPE': security tools and legal support that employers should provide to staff facing TFGBV; a concept cited from the 2025 UNESCO-FeCoMo Roundtable.
SDG	Sustainable Development Goal See International Frameworks section above.
STEM	Science, Technology, Engineering and Mathematics Academic and professional fields; retention of women in STEM pathways is identified as a specific casualty of TFGBV's radio silencing effect on Kenya's knowledge economy.
TFGBV	Technology-Facilitated Gender-Based Violence Any act of gender-based violence committed, assisted, aggravated, or amplified through the use of digital technologies, online platforms, or information and communication technologies. The central subject of this analysis.

Community Advocacy & Awareness (CRAWN) Trust
4th Floor All African Conference of Churches of Kenya,Waiyaki Way, Westlands.
P.O Box 943-00621, Nairobi, Tel: 020-2664505, E-mail: crawn@crawntrust.org